Developing a framework for the search and seizure of digital evidence by forensic investigators in South Africa

DC Myburgh

27414655

Dissertation submitted in fulfilment of the requirements for the degree Magister Commercii in Forensic Accountancy at the Potchefstroom Campus of the North-West University

Supervisor: Prof. JGJ Nortjé

5 December 2016

PREFACE

In 2013, I obtained my Bachelor of Commerce in Information Systems from the University of Cape Town titled “Search and seizure of evidence on trial in South Africa”. This research is a continuation of my study area and contains some adaptations of the core aspects of the first research done.

As an ex law enforcement officer and current digital forensics investigator, it has been my calling over the past 26 years to investigate transgressions and pursue offenders. As such, this research study was a constant struggle to maintain a balanced approach between recognising the rights of suspects and my natural inclination to benefit the rights of forensic investigators.

I would like to express my sincerest gratitude to the following individuals and acknowledge them for their positive impact on my life:

- To my wife and two daughters, I would like to apologise that my studies took up so much of our family time. You know you are my life, my love, the very soul of me and I thank you from the bottom of my heart that you were always my foundation, my support and my inspiration during yet another mountain I decided to climb.

- To my supervisor, Prof. Koos Nortjé, thank you for your guidance and for the many arguments we have had over the years to find the best solutions. Our arguments have always been in good spirit and have been some of my best learning experiences.

- Ilse Grobler, thank you for being my soundboard and the valuable guidance you have provided me with.

- My team at work, the Cyanreans, thank you for affording me this opportunity.

Most importantly, *Nomakanjane − omnia possum in Eo qui me confortat*. *Soli Deo Gloria*.

Key Terms

Digital search and seizure; off-site search of computers; seizure of whole computers; digital search and seizure warrants; legally privileged documents on computers; intermingled documents on computers; intelligibility of search and seizure warrants; digital evidence.

ABSTRACT

In cases involving digital forensics, lawyers and judges can find themselves reluctant participants when experts are testifying about the high-level technicalities of digital evidence. Litigators often find themselves in areas that are foreign to them being led by experts whose credibility they cannot assess. In addition, litigators often cannot validate their opinions or findings based on their own competencies (Kessler, 2010:2).

In 2002, Ball (2002:6) already observed that litigators could have been “damn good” litigators without knowing the inner workings of a computer in 1992, but by 2002 it was a ticking time bomb in practices without a sound knowledge of computers. A sound knowledge of computers also relates to judges, magistrates, law enforcement officers and forensic investigators in their respective fields.

Caloyannides (2003:89-91) together with Van Buskkirk and Liu (2006:25) independently stated that a significant number of judges who admit digital evidence also tend to make the unjustifiable leap in automatically assuming that digital evidence is reliable. This unwarranted high level of reliability assigned to digital evidence by the judiciary can be ascribed to their relative lack in relevant technical knowledge. Presiding officers can find themselves being blindly led by experts without a full appreciation of the impact that a small modification or alteration can have on the interpretation and credibility of evidence (Kessler, 2010:10).

In South Africa, very few cases were found where the technical aspects of digital evidence were thoroughly tested in courts. The outcomes of some of these cases were not positive for the State in that the search and seizures were set aside due to a number of unique difficulties that digital evidence pose to conventional search and seizure methodology and statutes. This setting aside of search and seizures can be attributed to the ill-advised application of out-dated physical world rules in a digital world (McLain, 2007:1076).

This study considered the reasons why search and seizure warrants for digital evidence were set aside internationally and in South African courts. Case law provides parameters on how courts interpret and provide guidance as to the acceptability of mechanisms employed by forensic investigators during search and seizures for obtaining digital evidence.

International guidelines were researched to establish how the unique complexities of digital evidence in search and seizures by global law enforcement agencies are managed while the fundamental principles of digital forensics, such as integrity and reliability of evidence, are maintained.

The research study proposes a framework for forensic investigators with regard to the search and seizure of digital evidence, which adheres to the parameters of the South African legislative framework. Although the study is limited to search and seizure under auspices of search and seizure warrants in terms of the provisions of the Criminal Procedure Act (51 of 1977), the parameters found can be applied to all regulatory statutes, which mandate the inspection, search or seizure of data − privately, departmentally and civilly. This study, therefore, addressed all law enforcement officers, government inspectors/investigators and fraud investigators as forensic investigators.

The proposed framework sets out the grounds for why the seizure of computers containing all data should be permitted and provides a comprehensive approach for forensic investigators to position authorised officers to apply their mind when evaluating if sufficient ground exists to permit the required infringement of the rights of suspects. The framework shows that although search and seizures are permitted, strict measures should be employed to ensure that forensic investigators do not gain access to more data than authorised in terms of search and seizure warrants.

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1 − INTRODUCTION

1. INTRODUCTION

With the inception of a digital age, South African courts had to adjust to accommodate a totally new notion of information − data. Data defies human senses. Data cannot be smelt, yet exists all around us. Data cannot be seen, yet have considerable value. Data cannot be touched, yet it can be stolen. Data cannot be heard, yet it serves as the communication medium of the masses (Kraidy, 2008:2).

If one considers Internet-related statistics from Internet World Stats (2015), statistics support this proliferation of technology in all strata of society and our daily lives (Welty, 2011:1). Devices, such as computers, laptops, tablets and cellular phones, have become ubiquitous (Kessler, 2010:24). With this proliferation of technology, the ease of use, low costs involved and the potential of anonymity and pseudonymous activities, have made it appealing to criminals − as recognised by the South African Law Reform Commission (2010:7) (hereafter referred to as the SALRC). As such, these devices have become a growing source of evidence in criminal and civil matters. Casey (2011:7) provides recognition to this "new type" of evidence, namely digital evidence − electronic information created on computers that can link crimes with suspects.

1.1 Background to the research area

Since 1976, when a court disallowed bank records created by a computer as evidence in the Narlis v. South African Bank of Athens (1976) case, South African courts have been faced by the foreignness of data. The SALRC (2010:7) acknowledges that ever since this case occurred, rapid developments in technology resulted in significant changes to the physical nature of computers, network technology, communication and a range of applications. However, law developments cannot keep pace with these rapid developments in technology (Nieman, 2009:3).

If the crime statistics in South Africa over the past few years (South African Police Service, 2016) are considered and the advent of computers in the commission of crimes is recognised − either as targets of crime or used as tools to commit crimes (Welty, 2011:1) − one needs to recognise the fact that in South Africa, search and seizures are performed on a daily basis (Basdeo, 2012a:164). It is, therefore, reasonable to accept that the point has been reached

where digital information is searched and seized on a daily basis to identify and obtain digital evidence as part of criminal and civil judicial proceedings (Bartholomew, 2014:1027). Casey (2011:6) states that computers are so ever-present, it should be collected as evidence routinely during search and seizures. The need to correctly collect, preserve and present digital evidence is not only of paramount importance to combat crime, but is essential for international cooperation as stated by the Committee of Ministers to member states concerning criminal procedural law connected to information technology (Council of Europe, 1995:3).

In 2002, the Electronic Communication and Transaction Act (25 of 2002) came into effect whereby judicial recognition was given to the concept of data and legal requirements for digital evidence were defined. The Electronic Communication and Transaction Act (25 of 2002) is relatively new and very little case law exists to define the interpretation of the various aspects of this Act. Nieman (2009:3) maintains that technology is known to oppose legal concepts − a thought supported by the SALRC (2010:7). The interpretation of the complexities of the Electronic Communication and Transaction Act (25 of 2002) concerning the complications that digital evidence brings to the South African courts has been left to individual case-by-case interpretations and very limited case law is available in this regard. The law is, therefore, interpreted without considering the unique nature of digital evidence involved, which impacts directly on the formulation of investigative procedures. These interpretations can only be tested in a court of law when the defence, the prosecution and presiding officers understand, argue and assess all aspects relating to digital evidence in cases. Hofman (2006a:274) asserts that detailed procedures are missing, and proposes that there should be procedures that can be scrutinised and accepted in court. Hofman (2006a:18) further suggests that courts are in need of expert assistance to understand the technical requirements of digital evidence and digital forensic procedures.

The following quote from William Pitt (1763), dating from the 17th century, emphasises the importance for the State to protect and respect the right of individuals with regard to their privacy:

> *The poorest man may, in his cottage, bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England may not enter; all his force dares not cross the threshold of the ruined tenement.*

It is in the area of searching for and the seizing of digital evidence that the technical nature of digital evidence and the expectations of privacy associated with digital devices versus the

interpretation of the South African law, specifically come to the forefront. One of the first technical aspects tested in South African courts was the creating of a forensic duplicate of the computer containing all the data and performing an off-site analysis. This is the practice in large parts of the world (Kerr, 2015:1). This was questioned in the Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) case when computers were removed from the scene.

The aim of this research study was conceptualised by the following specific judgment of the court in the Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) case:

> *As to the allegation by the respondent that this "has become the standard way of searching for electronically stolen information in South Africa and elsewhere in the world", if this is so, it, in my view, not sanctioned in South Africa by Sections 20 and 21 of the Criminal Procedure Act. There is nothing in these Sections in terms of which anything which is not "an article referred to in Section 20" may be seized or removed from where it was found. It was in any event unnecessary for the police to remove these articles from the South African applicants' premises. The electronic data found by the police at Mowbray could effectively have been searched and copied at the premises within a few hours, using technology which is readily available.*

1.2 Literature review

The research of available literature indicated that many of the technical aspects of digital forensics as a science were discussed academically during the late 1990s to the early 2000s when the science of digital forensics started to take shape. These aspects were discussed and argued by scholars and the literature found is still relevant and accurate today. Although some of the reviewed literature is dated, no publications were located that refute or substantiate these assertions, and older literature is, therefore, found to still remain the most current literature. Kessler (2010:12) was frustrated with the lack of academic research in this area and states that although digital forensics has been an area of active investigative practice during the past years, the use of digital evidence in courts is still limited and that the field is still a new academic discipline.

Newer implications and arguments originated from case law when technicalities and law meet. The ruling of the court in the Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) case is an excellent example, which was also the starting point of research from which

keywords were derived to locate information on the topic. This study focused on the most prominent issues pertaining to the search and the seizure of digital evidence in South Africa.

The judgement of the court in the Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) case, as discussed above, begs that clarity be obtained regarding the remarks of courts in relation to what has "become the standard way of searching for electronic(ally) (sic) stolen digital information in South Africa and elsewhere in the world", what is "sanctioned by Section 20 and 21 of the Criminal Procedure Act 51 of 1977" in relation to the removal of digital evidence "from where it was found" and how can digital evidence be "effectively searched and seized".

Preliminary research identified that there is limited research in South Africa available on this subject. Limited research includes research studies by Nieman, Basdeo and Bouwer from 2006 to 2014. There is also limited South African case law available in this area.

The study was, therefore, extended to international sources due to the limitation of available information on this subject in South Africa. This was done mainly in similar legal environments in which relevant cases and aspects were argued on the same legislative basis. Literature from Canada, the United Kingdom, Australia, New Zealand and the United States of America was preferred.

1.3 Motivation of actuality

The study was limited to the search and seizure of digital information under auspices of search and seizure warrants in terms of the provisions of the Criminal Procedure Act (51 of 1977), but the principles found can be applied to all regulatory statutes, which mandate the inspection, search or seizure of data. It was established that there are a number of organisations with an inspection or investigation function in South Africa under various authorisations and/or legislation. The correct handling of digital information and evidence can be beneficial to various organisations due to the increase in the use of information technology:

- South African Police Service (hereafter referred to as the SAPS)
- Auditor General
- South African Receiver of Revenue

- Competition Commission
- Health Profession Council
- Financial Services Board
- South African Secret Service
- Special Investigation Unit
- Cyber Inspectors
- Sheriffs of the Court
- Execution of Anton Pillar orders.

Judges play a gatekeeper role in determining what scientific evidence is accepted in their courts (Kessler, 2010:100). Just as judges need to eliminate junk science from court cases, they also need to keep out digital evidence of poor quality (Kessler 2010:6). It was found in this study that few reported cases to date have been argued on the technical aspects of digital evidence in South Africa and that in very few cases where digital evidence was presented, the evidence was questioned. During an informal discussion with a member of the SAPS, the comment was made that it is not necessary for them to change their methodology, since they are not losing too many cases in this regard. However, from available literature it is evident that in the cases studied in which the conduct of the SAPS was thoroughly examined, the rulings were largely in the favour of suspects. Neufeld's (2005:4) statement is sad, but true − if nobody questions speculative science, there is nothing for gatekeepers to tend to.

Galves and Galves (2004:2) contend that forensic investigators are more inclined towards the collection and investigation of non-technical evidence. This is mainly due to a lack of knowledge and resources on how to deal with digital evidence (Craiger & Shenoi 2007:49). If the South African criminal justice system − due to a lack of knowledge and resources − fails to hold criminals accountable for their actions based on improper procedures, such as incorrect search and seizure procedures, criminals will perceive themselves as untouchable by the law. In the landmark case S v. Makwanyane and Another (1995) in which the death penalty in South Africa was found to be unconstitutional, the court stated that the greatest restraint against crime is the

expectation that offenders will be reprimanded. The court also stated that this is precisely what is lacking in the South African criminal justice system.

The court's ruling in the Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) case found amongst other things that the seizure and removal of the computer containing all of the data from the scene infringed the rights of the suspect. The ruling of the court was further re-enforced in the recent case of Imperial Crown Trading 289 (Pty) Ltd v. Birch NO and Others (2012) where the Northern Cape High Court ruled that the search and seizure of computers − where the computer containing all of the data was copied and seized − was too broad. In the case of Smit and Maritz Attorneys and Another v. Lourens No and Others (2002), an external digital forensic investigator assisted the SAPS on the scene to conduct a search of the computers and this was found to be unauthorised. This ruling further restricts the SAPS to only make use of internal digital forensics investigators on scenes.

In all three above-mentioned cases, the court instructed the SAPS to hand back the seized evidence or a portion thereof due to the fact that the search and seizure warrant and the subsequent execution thereof were deficient. The value of this evidence was, therefore, lost to the State's case. While the rulings were not appealed by the State, the SAPS also did not adjust their search and seizure methodology. The most current National Instruction on Search and Seizure was issued in 2002 (SAPS, 2002). In this instruction, no mention is made of computers, cellular phones, social media or cloud computing. In 2016, the National Instruction has been supplemented by the Practical Guide to Apply for Search Warrants in terms of Section 21 of the Criminal Procedure Act (51 of 1977) (hereafter referred to as the SAPS Practical Guide).

Hopefully, this study will assist the SAPS and related organisations in compiling instructions on what the most acceptable processes are to follow in searching and securing digital evidence to both serve the interests of justice and the rights of suspects.

1.4 Problem statement

The literature review identified a number of unique aspects that digital evidence pose to traditional search and seizure practices. The research problem statement was amalgamated in three primary research questions:

- How should search and seizure warrants for digital evidence be structured in South Africa?

- How should search and seizure warrants be executed to protect the rights of suspects and to serve the interests of justice?
- How should definitions relating to search and seizure concepts be interpreted in relation to computer-related aspects?

1.5 Objective

1.5.1 Main objective

The above-mentioned problem statement that was divided into three primary questions can be combined into the main objective of developing a framework for the search and seizure of digital evidence in South Africa by forensic investigators.

1.5.2 Secondary objectives

In order to reach the primary objective, the following secondary objectives were addressed:

- To provide guidance on the correct structure of search and seizure warrants for digital evidence.
- To determine the correct methodology of executing search and seizure warrants for digital evidence.
- To determine the correct use and interpretation of digital forensics terminology.

1.6 Hypothesis

It is possible to develop a framework for forensic investigators in South Africa with regard to the correct use of search and seizure warrants for digital evidence, for these warrants to contain the correct terminology, and to set out the correct approach and structure for search and seizure warrants for digital evidence.

1.7 Research design and method

This quantitative research was planned based on a strategic framework, which allowed for the implementation of the research in an organised fashion to meet the research objectives in the form of a cross-sectional design by combining a literary review with an empirical study in the form of unstructured interviews.

1.7.1 Qualitative research

A qualitative study focuses primarily on exploratory research to gain an in-depth understanding of opinions, interpretations and motivations to provide a deeper insight into a problem and to assist in developing ideas or a hypothesis (Wyse, 2011). The advantage of a qualitative study is that it is more dynamic, it can be more easily adapted and is not defined in pure technical terms (Terre Blanche *et al*., 2010:35). Internationally, the field of digital forensics is a relatively new academic research area (Kessler, 2010:12). The research was, therefore, largely exploratory and it was necessary to consider a wide field of literary to ensure that the field of research was sufficiently covered (Terre Blanche *et al*., 2010:289). The use of limited case studies in the form of unstructured interviews were sufficient in establishing policies and procedures, which is being followed by the SAPS and Competition Commission of South Africa in relation to the search and seizures of digital evidence (Terre Blanche *et al*., 2010:289).

1.7.2 Literary review

The literature review sought to discover relevant sources pertaining to the research area. Although Webster and Watson (2002) are of the opinion that there is still significant confusion regarding the structure and format of a literature review, it is clear that the main aim of a literature review is to summarise information regarding a research area that supports the documentation of detailed research questions. Serra (2015) maintains that a literary review forms an integral part of any academic research. It shows the reader that the researcher conducted a comprehensive study of the field. Terre Blanche *et al*. (2010:21) highlighted some of the prerequisites of conducting a literary review:

- Care should be taken that a wide array of relevant sources are studied.
- Information should be accurate and appropriate.

- Pertinent material should be highlighted.
- A literary review should contribute to the pool of knowledge.
- Focused reading should be provided on the topic.
- A literary review should be well-structured and systematically presented.

Care was, therefore, taken to address these prerequisites by focusing on the legislation governing criminal search and seizure, such as the Criminal Procedure Act (51 of 1977) in South Africa or equivalent legislation in other countries. The main focus of the study was, however, on case law, which provided the purest indication of how courts currently interpret legislation and what problems are experienced globally in this area and how these problems can be addressed in a South African context. From a preliminary literature assessment, it was evident that the most prominent cases originated from the United Kingdom, Canada and the United States of America. The focus of the study rested mainly on these countries and on South African case law. The literature used consisted of:

- Approved and draft legislation
- Academic papers
- Case law and court transcriptions
- Peer-reviewed articles
- Court rulings
- Law Commission reports
- Subject-relative books.

1.7.3 Unstructured interviews

Unstructured interviews can be compared to free flowing conversations (Sravani, 2016) and these interviews can be adapted in real-time while the framework of the research can be adapted as new information is discovered (Occupytheory, 2014). McLeod (2014) identified some of the advantages on unstructured interviews:

- Questions can be amended in accordance to the answers received from interviewees, because they are free flowing.
- Questions allow interviewees to discuss answers comprehensively, which can assist researchers to understand situations better.
- Validity is increased, because these interviews allow researchers to probe deeper for a better understanding and to clarify aspects.

Sravani (2016) is of the opinion that unstructured interviews can lead to discussions of confidential information and can be time-consuming. These disadvantages were managed by obtaining approval for the use of information and the number of interviews was limited since only information regarding procedures was required.

Unstructured interviews were required to establish what processes are currently followed due to the fact that the policies and procedures of the SAPS and the Competition Commission of South Africa are not available to the public domain. An unstructured interview was conducted with a former police officer who is an expert in digital forensics and was part of the management of a digital forensics unit of the SAPS (Anon, 2016a). The aim of the interview was to establish what the current process is within the SAPS in relation to the search and seizure of digital evidence. A second unstructured interview (Anon, 2016b) was conducted with an advocate working with investigations concerning the Competition Act (89 of 1998). The interviews were limited to one individual per area since the objective was to establish what the policy and procedures are within the SAPS and Competition Commission of South Africa in relation to the search and seizures of digital evidence. Only two interviews were conducted, because additional interviews would not have discovered any new information since the interviews were limited to discovering information relating to policies and procedures. Atlas.ti is an invaluable tool during the collection and processing of interview data. However, Atlas.ti was not used due to the fact that the amount of interviews was limited and Atlas.ti could not contribute more value to this study.

1.8 Ethical aspects

Ethical standards are of the utmost importance during academic research. Resnik (2015) defines ethical standards as norms of behaviour that distinguish between acceptable and

unacceptable conduct and the author further states that maintaining ethical behaviour in academic research:

- Promotes the aims of research, such as accuracy, truth and knowledge.
- Promotes trust, respect and fairness during collaborative research.
- Protects intellectual property.
- Promotes accountability of researchers towards the academic and general community.

The research topic was approved by the colloquium of the North-West University, Potchefstroom Campus, and the study adhered to the ethics requirements in order to maintain quality, confidentiality and anonymity.

In conducting the study, the researcher attempted to take into account all relevant ethical considerations, especially in relation to the freedom from physical or psychological harm and disclosure about the nature of the research or privacy. Participation in the unstructured research interviews took place on a voluntary basis and the identity of the interviewees was kept anonymous while all personal information will also be kept confidential.

1.9 Terminology used

Some of the specific terminology concerning digital forensics is more broadly defined in later chapters. For the purpose of this study, the following general terminology has the following meaning:

Authorised officers – persons authorised to issue search and seizure warrants. In South Africa, this function is performed by judges, magistrates, regional court magistrates and justices of the peace.

Courts − can refer to judges and/or magistrates depending on the context.

Digital forensic investigators – persons qualified and responsible for conducting digital forensic investigations.

Forensic duplicates – refer to the term "forensically sound duplicate original records" and include copy and mirror images.

Forensic investigators – refer to investigators with legislative authority to conduct searches and seizures.

Search – based on a specific context, the reference to *search* is divided into one of the following three distinct phases: The first is the traditional process whereby forensic investigators look for or locate physical computers on a scene. Secondly, forensic investigators search for or segregate relevant and non-relevant information/data on computer and lastly, the analysis or interpretation of relevant information within the context of a larger investigation.

Traditional search and seizure – reference is made to search and seizure prior to digital evidence where the focus was on documents or physical articles.

1.10 Overview of chapters

Chapter 1 Chapter one contains the introduction, background to the research area, motivation of actuality, research design and the methodology followed, the literature review, problem statement, objectives, hypothesis and the meanings of some of the terminology used in the study.

Chapter 2 In chapter two, an overview is provided of computer hardware and software and the structure of data to provide the reader with baseline knowledge. This chapter highlights some of the technical complications, which digital devices pose to traditional search and seizure.

Chapter 3 Chapter three considers the terms and concepts concerning digital forensics and the search and seizure of digital evidence.

Chapter 4 Chapter four provides an overview of the leading international standards and guidelines applicable to digital forensics and presents the international industry requirements for digital evidence.

Chapter 5 In chapter five, the legislation impacting on search and seizure in South Africa is discussed with reference to international treaties.

Chapter 6 In chapter six, an in-depth research discussion takes place of internationally identified areas where digital evidence contradicts or complicates traditional legal approaches. These areas and the results of the unstructured interviews are discussed in relation to international and local case law.

Chapter 7 In chapter seven, a summary of the study is provided with conclusions, recommendations and identified new research areas based on the findings from the research. These conclusions, recommendations and new research areas are considered when deciding whether the hypothesis was proven correct from the research.

CHAPTER 2 – BASIC STRUCTURE OF COMPUTERS AND DATA IMPACTING ON DIGITAL FORENSICS

2. INTRODUCTION

The discipline of digital forensics requires a combination of skills, qualifications and knowledge in the area of forensic investigation, legal aspects and information technology (Kessler, 2010:1). A certain level of knowledge is, therefore, required in relation to computer architecture, operating systems, file systems, software engineering and computer networking to fully understand and argue the perceived contradictions or complications that digital evidence poses to the legal environment (Kessler, 2010:2).

In this chapter, a limited number of concepts − important for understanding the implications, specifically to the search and seizure of digital devices – are examined to lay a foundation for subsequent discussion. A distinction is made between tangible hardware or physical devices and intangible data consisting of programs, applications and information. This distinction is important since it will also play a role in later chapters to show that South African forensic investigators should make a distinction between the two classes of items since different legal aspects apply to both. This distinction forms the basis of Kerr's (2005b:85) suggested "two-step" search process that was adopted in the United States Federal Rules of Criminal Procedure, Rule 41, Search And Seizure (2009). Bouwer (2014:170-171) recommends the recognition and implementation of this approach in a South African legal environment, whereby forensic investigators first search for and locate physical devices ("search one") and then access and search these physical devices for relevant information or data ("search two").

An overview is provided regarding tangible devices or computer hardware. The emphasis is on physical devices that normally contain evidential data and are, therefore, usually the focus of "search one" during a search and seizure operation.

Secondly, an overview is presented of intangible data − the focus of "search two" and slightly more complex. The aspects addressed include: the structure of data, structure of a computer environment, metadata, data sizes and what complications the structure of data pose to search and seizure.

2.1 Computer hardware

Computer hardware consists of many types of devices and is ever-evolving. Devices include inter-alia personal computers, laptops and network devices, such as servers and routers

(Kessler, 2010:2). It can also be external or portable storage devices, such as memory sticks, external hard drives or mobile devices like cellular phones, tablets or IPads (Casey, 2011:01). The examples and case studies used in this study focus mainly on the personal computer environment.

Woodford (2007) explains that computers are electronic devices that primarily process data. Computers mainly consist of an input device, such as the keyboard, a processor or the central processor unit, a data storage device, such as the hard drive, and an output device, such as a printer or screen.

2.1.1 The evidential value of computer hardware

Physical devices are normally not of interest to forensic investigators (Health and Safety Executive, 2014) other than to submit for fingerprint and human DNA analyses or if these devices are stolen items. Normally, the real importance of these devices is contained in the data that are stored on these devices. During investigations, the data storage devices are predominantly the articles of interest for forensic investigators and it is often practice to specify these devices as the articles to be seized. Kessler (2010:2) identifies a number of these physical devices:

- Hard drives
- Memory sticks
- External hard drives
- Data tapes
- Cellular phones
- Ipads
- Tablets
- Secure Digital Cards (SD cards)
- Compact disks (CDs)
- Digital versatile disks (DVDs).

2.1.2 The importance of computer hardware in relation to search and seizure warrants

In South Africa, the State focuses on describing computer devices and data storage devices in detail when search and seizure warrants are issued. A typical example was located in the case of the National Director of Public Prosecutions and Others v. Zuma and Another (2008):

> *… electronic computer data includes computers, laptops, stiffies, hard drives, compact discs, data cartridges, backups, electronic devices and any other form in which electronic information can be stored or saved.*

One of the main constraints or complications emanating from digital devices is the variety of devices available − digital forensic investigators should be able to accommodate them all. A large portion of these complications stems from the proliferation of mobile devices. Statista (2016) reports that cellular phone users have grown globally to 4,61 billion in 2016. According to Jain (2015), three different types of cellular phones were launched daily in the Indian market during 2014. Coupled with this, hard drive manufacturers are continually trying to improve hard drives by increasing the storage space and speed of these drives. Seagate (2016) reports on the different varieties of connectors used in creating the newest hard drives. It is expected of digital forensic investigators to continually maintain cutting-edge technology to be able to connect to these different devices to be able to extract evidential data from them.

2.2 Data and software

Collecting digital evidence is far more complex than collecting physical evidence (Casey, 2011:8). A part of this complication is the fact that data consists of electric impulses that can be transmitted at an instant, stored at any location in the world or distributed to many different locations, destroyed in a second and modified or altered if handled incorrectly (Nieman, 2009:19).

2.2.1 Structure of data

Data is stored as magnetic “on” or “off” impulses, normally on the hard drives of computers (Kerr, 2005a:539). Hard drives are physical devices, as described above. Traditional hard drives consist of several magnetised metal platters − metal compact disks upon which the magnetic impulses are stored. If these magnetic impulses are positively stored, these impulses are represented as a “1” and if these magnetic impulses are negatively stored, these impulses are represented as a “0” (Kerr, 2005a:539). These magnetic impulses are referred to as a binary code (Guzzi, 2012:301). A binary code forms the building blocks from which all words, documents, programs or operating systems are built. Computers do not, therefore, store

physical words, but would store, for example, the word “CAT” as the following binary code: “01000011” = C, “01000001” = A and 01010100” = T (Binary Translator, 2016).

It is very seldom necessary for digital forensic experts to explain data down to this technical level during court cases. This example is provided to show how volatile data can be and in subsequent chapters how the integrity of data is assessed.

For the purpose of this research, the definition of “data” is applied as an adaptation from Section 1 of the Electronic Communication and Transaction Act’s (25 of 2002) as the digital representation of information in any form and not the “electronic representation of data in any form”.

Computers can store massive amounts of data (Lowenstein, 2007:7). In the Matter of the United States of America’s Application for a Search Warrant to Seize Electronic Devices from Cunnius (2011:6), the court recognised that a single gigabyte of data can contain 500 000 double-spaced pages of text. The average size of a hard drive is 1000 Gigabyte (GB) or one Terabyte (TB) with up to 16TB hard drives available. A 1TB hard drive can, therefore, contain 500 million double-spaced pages of information. To trawl through or review this amount of data can be very labour-intensive and time-consuming.

Suspects can further easily frustrate a search (Lowenstein, 2007:8) by encrypting, hiding or deleting data (Bartholomew, 2014:1035). Even if forensic investigators know what to search for, it can be a very time-consuming process. It can literally take weeks to locate information specified in search and seizure warrants (Bartholomew, 2014:1035).

Vandeven (2014:2) explains that once users delete files, those files are sent to an “unallocated space” on computers. In the Matter of the United States of America’s Application for a Search Warrant to Seize Electronic Devices from Edward Cunnius (2011:8), the court stated that while physical documents can easily be removed from filing cabinets, digital evidence cannot be so easily removed or destroyed and can be recovered − months or even years later. This statement has both a positive and negative impact on digital forensic investigations. On the positive side − even if suspects destroy data, there is a viable chance to recover evidence. On the negative side − if persons have legally privileged information on their computer and they delete this information to prevent the police from seizing it, this information is still discoverable via data recovery.

Other aspects that can also complicate investigations for forensic investigators are cloud computing, online data storage and social media. In the Matter of the United States of America’s Application for a Search Warrant to Seize Electronic Devices from Edward Cunnius (2011:7), the court recognised that computers are not only repositories of data, but can also be access

points or portals to data stored at any location worldwide. Pickering (2009) provides a simplified description for cloud computing as a pooled number of computer resources provided over the Internet or World Wide Web. It involves the interaction of several servers, interacting and functioning as a large virtual server "pool" that can expand or contract depending on requirements. Social media is undoubtedly one of the fastest growing, most popular and most influential powers in our current digital environment. According to Smith (2016), there are 3,17 billion Internet users worldwide with 2,3 billion social media users. Currently, there is very little standardisation of investigation methodology with regard to social media investigations (Mulazzani *et al*., n.d.) The existence of these online storage sites or social media profiles can be unknown prior to a search and seizure operation and can, therefore, pose jurisdictional issues in obtaining search and seizure warrants. Traditional digital forensics relies on the creation of physical forensic duplicates of whole hard drives and hash analyses to indicate the integrity of evidence. This issue is explained in more detail in later chapters. The creation of physical forensic duplicates of whole hard drives and hash analyses does not always apply to the social media or a cloud forensics environment, which can be dynamic and a live investigation then takes place where some investigation functions are performed on the actual original data.

2.2.2 Software structure on computers

Computers need an operating system, such as Windows XP, Windows 8 or Windows 10, which organise and control how all hardware and software operate (Franklin & Coustan, n.d.). Additionally, computers have programs or applications, such as Word or Excel, which enable users to create and edit documents.

A simple differentiation − used later throughout this study to differentiate between classes of data − is to classify information or files on computers as follows:

- *System files* − all the program and application files needed to operate a computer and these files form part of a default installation on a computer. Word, PowerPoint or Excel are examples of system files.

- *Computer-generated records* − all files generated by a computer (untouched by human hands) but altered or recorded as a result of human activities. Log files, the Internet history or registry files are examples of computer-generated records.

- *Computer-stored or user-created records* − all data that are created by users on a computer. Spreadsheets, emails or documents are examples of computer-stored or user-created records (Nieman, 2009:7).

Typically, investigators are only interested in data created by users or as a result of the activities of users and not the generic system or program files. An exception occurs if hacking is investigated and the programs used by perpetrators are of importance. Generally, normal off-the-shelf programs on computers are not of interest to investigators during investigations.

An operating system keeps a significant amount of information with regard to the use and functioning of computers – the setup of computers, the users and the activities taking place on computers. This information is kept within the registry or system/program files of computers (Gookin, n.d.) and kept separate from user-created data and can contain valuable evidence (EC Council, 2004:75), such as who worked on a computer and what the person did. The operating system also keeps additional information on the files of users, such as locations, file names and more in the file allocation table and master file table (EC Council, 2004:85-94). This information is pertinent in investigations to establish when files were created or moved.

Computers also keep information imbedded inside files and folders, such as when files were created, edited, printed, who were the authors of documents and a magnitude of other information. This information is kept as metadata and embedded within documents (Kerr, 2005a:542). Users cannot see this information within the content of documents, but can access some of this information by accessing the “properties” of files. Metadata plays a crucial role in digital forensics. Ruhnka and Bagby (2008:68) refer to metadata as the equivalent of electronic DNA. Metadata can prove a person’s guilt or innocence and also one of the easiest ways to verify the originality, integrity and authenticity of documents (Ball, 2011:2). Examples of the various locations that can yield information or metadata regarding files, include the master boot record, the master file table, the operating system, the registry, and within the applications or software. These areas are depicted in more detail in Figure 1 below. As can be seen in this Figure, a magnitude of information is kept at different locations on computers − separate from the files in question.

As a science, digital forensics does not yet have the advantage of established longevity, which other forensic sciences have built up over years (Vacca, 2005:237) but increasingly used more often in courts, more of the “weaknesses” and “strengths” of the digital forensics science will become known (Nieman, 2009:21). Just with human DNA, litigators are becoming more knowledgeable on the subject and weak or improper evidence will be questioned and weaned out (Plowden & Stockdale 1998:432).

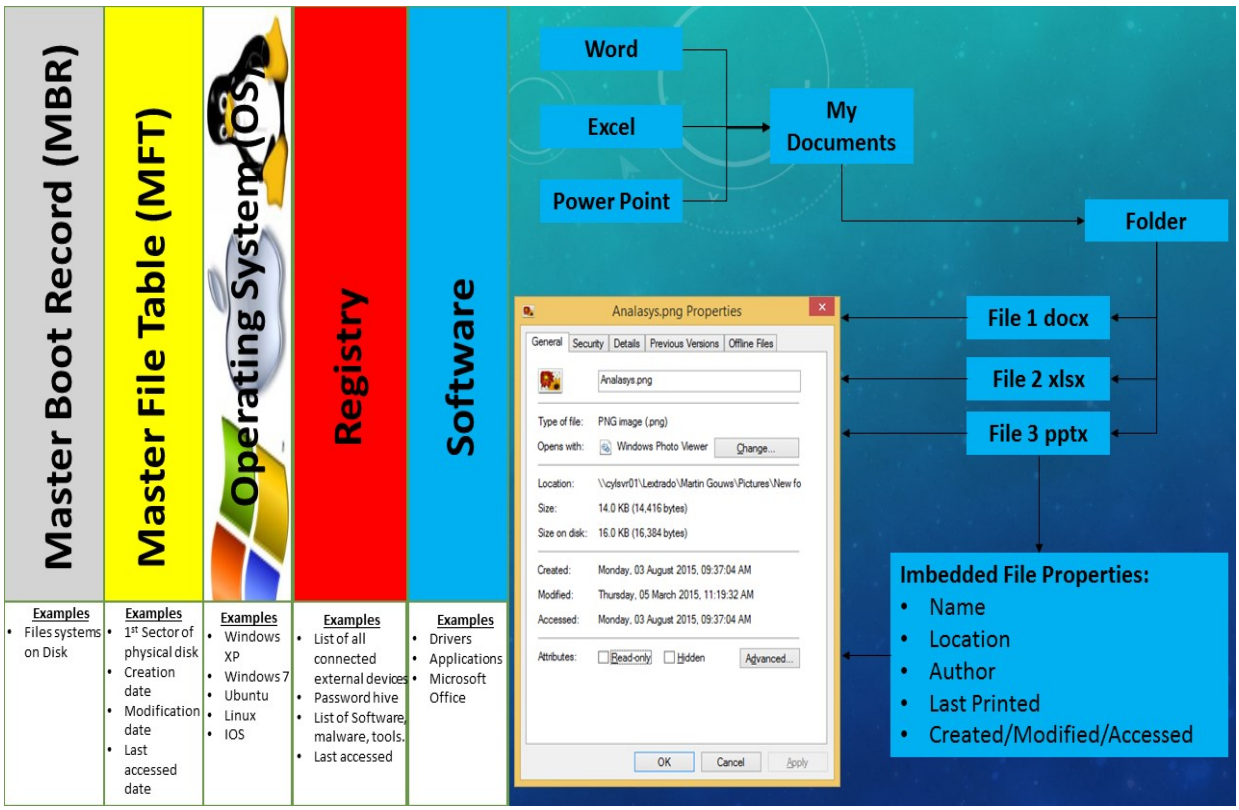

Figure 1 – Structure of data and an example of where metadata is available at different locations

Significant to this research study, was the fact that although the main interest of investigators in computer data relates to the activities or files of users, important significant evidential data regarding the activities of users or files are kept on different locations on computers. If investigators only seize, for example, child pornographic images from a computer, which are computer-stored records, without taking any system files or computer-generated records, there can be a multitude of aspects they would not be able to examine or prove. These aspects include not being in a position to determine or prove how the files came to be on the computer, who had access to the computer and who knew about the existence of these files. These aspects can also leave forensic investigators powerless against the defence making claims emanating from information purportedly originating from portions on a computer, which they were not allowed to forensically duplicate or analyse. Claims made by the defence can include the presence of malicious programs on computers that downloaded the pornography without the knowledge of users or that users were hacked. If forensic investigators are not permitted to forensically duplicate and analyse computers containing all of the data – investigators cannot, therefore, locate and examine evidence pointing away from the guilt of suspects. (British Attorney General, 2013:24).

2.3 Summary

It is evident in this chapter, that the uniqueness of digital evidence poses complications to traditional legal approaches. Digital evidence encompasses both tangible devices and intangible data and requires special methodologies to identify and collect all relevant evidence. The seizure of all data on computers can be viewed as overbroad due to the fact that not all of the relevant information is contained within files, but can reside on different locations on computers. The technical nature of cybercrimes and subsequent technical expert testimonies add further dynamics that are faced by digital forensic investigators. In the next chapter, various terminologies specific to the search and seizure of digital evidence are discussed in the context of legal interpretation.

CHAPTER 3 – TERMINOLOGY

3. INTRODUCTION

During the research study, it was found that in many academic papers and court cases, information technology terminology is used interchangeably without any regard to being unambiguous and consistent in the interpretation of terminology in relation to legal texts. This mainly contributes to the fact that information technology terminology is unknown in the legal system (Kessler, 2010:2). Many of the information technology terms or concepts have not yet achieved legal recognition. This notion is supported by the SALRC (2010:8), who expressed the opinion that many of the earlier held opinions that computers are "just like" filing cabinets, do not hold true in light of new technological capabilities. This was also the opinion of the Supreme Court in the Canadian case in R. v. Vu (2013).

Accurate legal definitions are vital to the operation of legal instruments and refer to words signifying concepts in law and consist of technical or legal terms and non-technical terms from ordinary language use (Jopek-Bosiacka, 2011:9). The meaning or interpretation of many words used in legal discourse is derived from ordinary language, but the true development of legal terminology − to a great extent − is derived from legal discourse in courts and depend less on the parameters set for communication with regard to generally recognised legal science principles (Jopek-Bosiacka, 2011:10, 14). The recognition of terminology in a legal context is of the utmost importance to ensure that miscommunication does not occur. One should bear in mind that an initial understanding of texts may not be the only plausible interpretation (Clark & Connolly, 2006:2). This can especially be true in a digital environment where technical aspects can have an influence on the normal interpretation or understanding of concepts. Already in 1995, a longstanding supposition was noted by Sarkowicz (1995:91) that the interpretation of legal texts has one acceptable meaning. It would make it impossible for courts to pass any decision or judgment if legal texts have more than one acceptable meaning. Although one acceptable meaning is the ideal, the interpretation of legal texts cause frequent problems as the only meaning embodied in texts may not be the same for all addressees (Jopek-Bosiacka, 2011:14). In 1958, Hart (1958:607) encapsulated this issue perfectly by stating that in the most elementary form of law, the terms used should have some standard instance in which no doubt exist about their interpretation. Hart (1958:607) is of the opinion that there should be a "core of settled meaning".

In an attempt to provide clarity or guidance on some of the terms and concepts applicable to digital forensics and for the search and seizure of digital evidence, some of the concepts and terminology are reviewed and discussed. Using the Criminal Procedure Act (51 of 1977) as a

point of departure, this chapter focuses on a systematised introduction of relevant terms aimed at an explanation or interpretation of relevant terminology with the aim of assisting with formulating legal definitions.

3.1 Relevant legislation

3.1.1 Section 20 and 21 of the Criminal Procedure Act (51 of 1977)

Section 21 of the Criminal Procedure Act (51 of 1977) is the most relevant Section for the research study and relates to the power of authorised officials to issue search and seizure warrants, based on information supplied under oath, authorising police officials to enter a premises and search the premises or persons to locate identified articles and to seize such articles.

A Section 21(2) search and seizure warrant issued under subsection (1) shall empower a police official to seize the article in question and shall to that end authorize such police official to search any person identified in the warrant, or to enter and search any premises identified in the warrant and to search any person found on or at such premises.

The Section further therefore authorises the police official to search and seize articles:

- Which is concerned or on reasonable grounds believed to be concerned in the commission or suspected commission of a crime.
- Which may afford evidence regarding a crime or suspected crime.
- Which is intended to be used or on reasonable grounds believed to be used in the commission of a crime.

From this Section − as a point of departure − four concepts require further scrutiny on how these definitions relate to the digital environment and how these definitions should be adapted to apply to the digital environment, namely:

- The concept of *search*.
- The concept of *seize*.
- The concept of *articles*.
- The concept of *premises*.

An in-depth understanding of these basic concepts are required to fully understand how, and if, they apply to all aspects of the search and seizure of digital evidence. A comprehensive understanding is important for forensic investigators to ensure that all applications and executions of search and seizure warrants stay within the permitted ambit of the law. The intrusive nature of search and seizure warrants and the obligation of the judicial system to guard against the misuse of this authority are well-documented in the Constitutional Court Case of Powell NO and Others v. Van der Merwe and Others (2004). During this case, it was said that South African law has a long history of scrutinising search and seizure warrants with rigour and exactitude and that the common law rights are now enshrined in Section 14 of the Constitution (1996). Because of the danger of misuse during the application of authority with regard to search and seizure warrants, the judiciary scrutinises the validity of warrants with jealous regard for the liberty of suspects and their rights. This scrutiny applies to both the authority under which search and seizure warrants are issued and the scope of the terms listed in these warrants. The scope of terms are even more relevant in cases involving digital evidence due to the wide scope of personal and confidential information kept on the digital devices of persons (Guzzi, 2012:302).

The Explanatory Report to the Convention on Cybercrime of the Council of Europe suggests that additional procedural provisions are necessary in order to ensure that data can be secured in a manner equally effective as the search and seizure of tangible objects (Council of Europe, 2001b:32). This is firstly due to the fact that data is intangible – an electromagnetic medium. Secondly, while data can be read by making use of computer equipment, data cannot be taken away in the same sense as paper records (Council of Europe, 2001b:32). Kerr (2005a:533) captures some of the complexities of digital evidence as follows: “How can the old rules fit the new facts? For example, what does it mean to ‘search’ computer data, or when is computer data ‘seized’?” The Explanatory Report to the Convention on Cybercrime further suggests that to “seize data” can only be done in a number of ways, namely data can be printed and seized; the tangible medium upon which data is stored can be seized or a forensic duplicate should be made of the data and the tangible form upon which the copy is saved, should be seized (Council of Europe, 2001b:32). It is suggested that domestic law should provide for the power to create such duplicates (Council of Europe, 2001b:32).

3.1.2 Defining the search for digital evidence

If scenes are searched and computers are located, it cannot be concluded that the data on these computers have been searched. It is argued later in this study that a search of digital evidence should consist of a multi-step process as proposed by Kerr (2005b:85). Kerr (2005b:85) suggests that forensic investigators should first search for and locate physical

devices (“search one”). Then forensic investigators should access and search these physical devices for relevant information or data (“search two”). For the purpose of this study, references to “search” are extended from Kerr’s two-step process to include three phases, namely:

- The traditional process in which forensic investigators search for or locate physical computers on a scene.
- The forensic investigators search for or segregate relevant and non-relevant information/data on these computers.
- The analysis or interpretation of relevant information within the context of a larger investigation. This discussion of the definition of “search” relates to the later steps followed when data is searched, since it is acknowledged that the search for physical articles on a premises is well-defined and understood in the law.

The phenomenon of seizing taking place before a search has taken place, is supported by Brenner and Fredericksen (2002:82) who state that a search and seizures of digital evidence turns a normal search and seizure on its head in the sense that computers are normally first seized and then searched. In the case of the Minister of Safety and Security v. Bennett (2007), it was recognised that in instances where large collections of physical documents are located on a scene, and when it is impractical to separate or effectively search these documents on the scene, a broad seizure of the collection of physical documents is permitted, pending a later search to segregate relevant and non-relevant information. While an exception in relation to physical documents is made, the search and seizure of digital evidence due to the complexities of digital evidence poses a dilemma concerning traditional methods of search and seizure.

The Explanatory Report to the Convention on Cybercrime proposes that traditional words, such as “search” and “seize” should be replaced with more technological-orientated computer terms, such as “access” and “copy” (Council of Europe, 2001b:33). This proposal is supported by Nieman (2009:15) who is of the opinion that “search and seize” is more accurately described when computer terminology is used that is more neutral in meaning and can include actions, such as the creation of forensic duplicates of data. Currently, the proposed South African Cybercrimes and Cybersecurity Bill dated 19 June 2016 (2016) is not yet approved and will be submitted to the Cabinet in the last quarter of 2016. In the consultation document, the term “access” is included and is defined “to make use of, to gain entry to, to view, display, instruct, or communicate with, to store data in or retrieve data from, to copy, move, add, change, or remove data or otherwise to make use of, configure or reconfigure any resources of a computer device” (Cybercrimes & Cybersecurity Bill, 2016:6).

In the Minister of Safety and Security v. Xaba (2003) case, it was stated that the concept of "search" should be given its ordinary meaning. According to the *Oxford Dictionary*, "search" means "trying to find something by looking or otherwise seeking carefully and thoroughly" (Oxford Dictionary, 2016). The National Instruction 2/2002 of the SAPS (SAPS, 2002:1) states that "search" entails any action whereby a person, premise or container is visually or physically examined with the aim of establishing if an item or article is in, on or upon such a person, premises or container. However, Basdeo (2009:21) is of the opinion that this approach is questionable since "visually" is not defined and can include merely looking at something. Furthermore, the question of what constitutes a search is left to common sense − accessed on a case-by-case basis. Basdeo continues and argues that an element of physical intrusion is required to constitute a search of persons, premises or properties.

Based on the fact that data is non-tangible, it should be determined whether a physical intrusion takes place and if it constitutes a search when persons read, analyse or interpret data. In a physical environment, the reasonable expectation of the privacy of persons is breached when forensic investigators enter a premises. Merely observing a room does not constitute a fully-fledged search (Kerr, 2005a:536, 540). Kerr (2005a:547) proposes that an "exposure-based approach" should be adopted and that data should only considered to be "searched" when the data was exposed to human observation.

Basdeo (2012b:199) states that the Cybercrime Convention in Budapest (2001) (hereafter referred to as the Budapest Convention) constitutes the current international agreed upon benchmark for procedural powers in terms of digital evidence collection. The Budapest Convention proposes that "search" should include "to seek, read, inspect or review data", which includes the searching or examining of data (Council of Europe, 2001b:33).

For the purpose of this study, the interpretation of "search" as an "exposure-based approach" is supported and based on any action in which forensic investigators access data by whatever means and take notice of information or observe information in a humanly readable format. It is recognised that the term "search" is extraordinary broad and a differentiation is made for this study between the different contexts of search as an action to firstly, locate or look for devices on a scene; secondly, to locate and separate relevant and non-relevant data; and lastly, to analyse or interpret the data within the context of a larger investigation.

3.1.3 Defining the seizure of digital evidence

In the Rudolph v. Commissioner for Inland Revenue (1996) case, the court held that the term "seize" should be given its natural meaning. This ruling was supported in the case of Ntoyakhe v. the Minister of Safety and Security (2000) when the court held that "seize" means not only to

take possession of articles but also to retain them and according to Steytler (2004:84), to deprive persons of subsequent control over articles. Nieman (2009:16) adds that a seizure takes place when persons are deprived of their control over articles and without the subsequent right of retention of articles, the power of Section 21 of the Criminal Procedure Act (51 of 1977) is worthless. In the Ntoyakhe v. the Minister of Safety and Security (2000) case, it was cautioned that the right of retention is not unlimited and does not authorise the State to deprive persons of their lawful possession of articles indefinitely. This is a very important issue raised by the court. Although Sections 31 to 36 of the Criminal Procedure Act (51 of 1977) governs the disposal of articles under various conditions, no explicit reference is made to the duration in days when articles are retained from the point of seizure to when forensic duplicates are made or original articles are returned following the creation of forensic duplicates. The situation with computers differs from other classes of articles due to the fact that computers and other digital devices, such as cellular phones, play such a large role in our everyday life. The retention period under discussion is not the retention of forensic duplicates of computers during an analysis phase, but the period between the seizure of computers on a scene, the creation of off-site forensic duplicates and the subsequent return of original computers to owners. In many countries, legislation places a time period in days on this retention period. The retention aspects of digital evidence are discussed in more detail in chapter six. From an unstructured interview (Anon, 2016a), it was established that the practice in South Africa − due to limited resources − is that police officials in the majority of cases seize computers on scenes and then transfer articles to central digital forensic laboratories. During this interview, it was stated that some of the digital forensic laboratories are months − even more than a year − behind in their workload (Anon, 2016a). The interviewee (Anon, 2016a) estimated that on average persons are deprived from their computer (including cellular phones) for between five days to two years.

In light of the unique way in which digital evidence is normally collected or “seized”, Kerr (2005a:541) poses a number of questions with regard to the interpretation of when digital evidence is considered seized, namely:

- Does the creation of forensic duplicates constitute a seizure?
- Does the creation of forensic duplicates constitute a seizure of original evidence?
- If forensic duplicates are searched, does it constitute a seizure?

Kerr (2005a:557) states that these aspects are surprisingly difficult to interpret and at first sight it seems sensible to say that the creation of forensic duplicates constitutes a seizure of evidence. In the United States case of Arizona v. Hicks (1987), an investigator copied the serial number on a stereo system to verify later if it was stolen. The court held that the copying of this

information did not constitute a seizure. The court also held that the recording, copying or taking a photograph of information on a scene does not constitute a seizure. This finding highlights the question whether forensic duplicates of computers constitute a seizure. Kerr (2005a:560) further reviewed these complexities by arguing that if the creation of forensic duplicates is not recognised as constituting a search and seizure − since the data was not exposed, read or observed by humans, but only forensically duplicated − it can drastically expand the powers of the forensic investigators. In addition, Kerr maintains that should forensic duplicates not be viewed as a search and seizure, the forensic investigators would not need search and seizure warrants and Kerr refers to such a situation as "troublesome" and downright "creepy". Kerr urges that courts should apply the same principles to forensic duplicates of digital evidence than the principles applied to originals. Another consideration is what happens when forensic investigators bring an empty hard drive to a scene and creates a forensic duplicate of the suspect's computer. The hard drive was never a possession of the suspect, but remains an asset of the forensic investigators. It can, therefore, be argued that since the hard drive was never an asset of the suspect, it cannot be seized.

The Explanatory Report to the Convention on Cybercrime (Council of Europe, 2001b:33) proposes that "seize" should also include "to take away the physical medium which stores the data" or to make and retain forensic duplicates of data. This proposal is supported by Basdeo (2012b:199) who is of the opinion that the seizure of data not only includes the confiscation of data but also the "gathering" of data.

The concept of seizure is important to this study and it is, therefore, necessary to consider the way in which and the reason why forensic duplicates are created. A detailed explanation concerning the creation of forensic duplicates is provided in chapter four. Nieman (2009:22) explains that forensic duplicates do exactly what the name suggest − bit-by-bit exact duplicates of every sector of a hard drive are created. The requirement of Section 14 of the Electronic Communication and Transaction Act (25 of 2002) relating to the originality of evidence, stipulates that where the law requires information to be presented or retained in its original form, that requirement is met if the integrity of the digital evidence from the time it was first generated to its final form has passed assessment. The integrity of digital evidence is assessed by considering whether the evidence has remained complete and unaltered except for adding an endorsement or any change, which can be caused in the normal course of communication. Vacca (2005:237) states that a new concept of representational accuracy has emerged in terms of digital evidence − it is not necessary anymore to present the original. If forensic duplicates are created that depict the source data exactly, these duplicates can be considered originals. However, after forensic duplicates are created of computers and the originals are handed back

to suspects, as soon as a person switches on a computer − the content of that computer changes on a continual basis (Vacca, 2005:19).

The proposed Cybercrimes and Cybersecurity Bill provides a more inclusive definition for "seize" by including the rendering of data inaccessible, the removal of physical devices, to make or retain forensic duplicates or to make a printout of data (Cybercrimes and Cybersecurity Bill, 2016:9). For the purposes of this study, the interpretation of "seizure" includes the creation of forensically-sound duplicate originals and the seizure or retention of these duplicates is viewed by the State as originals.

3.1.4 Defining premises and containers

Section 1 of the Criminal Procedure Act (51 of 1977) defines "premises" as "including land, any building or structure, or any vehicle, conveyance, ship, boat or aircraft". It is questioned if this definition permits the inclusion of a computer as a premises and does this definition permit the search of computers prior to seizure? The SALRC expressed in their Discussion Paper on Computer Generated Crime (2002:14) the view that the provisions of the Criminal Procedure Act (51 of 1977) was developed prior to the notion that non-physical premises or non-tangible articles exist and the commission is of the opinion that chapter two of the Criminal Procedure Act (51 of 1977) does most probably not apply to the search of computers and the seizure of data located on computers. It was recommended that the Criminal Procedure Act (51 of 1977) be amended to specifically include the search of computers and the seizure of data. Section 82(4) of the Electronic Communication and Transaction Act (25 of 2002) stipulate, "For the purposes of this Act, any reference in the Criminal Procedure Act, 1977, to "premises" and "article" includes an information system as well as a data message". This would therefore apply to charges such as inter-alia illegal access to information and interference with data. Unfortunately, the new Cybercrimes and Cybersecurity Bill is silent in this regard and does not provide a wider, more inclusive definition, but recognises the searching of containers (Cybercrimes and Cybersecurity Bill, 2016:27). This definition is also supported by the National Instruction 2/2002 of the SAPS where it states that a search entails any action whereby persons, premises or containers are visually or physically examined with the aim of establishing whether items or articles are in, on or upon such persons, premises or containers (SAPS, 2002:1).

In 2012, the Seventh Circuit Court in the case of the United States v. Flores-Lopez (2012) defined containers as any objects containing anything else − including data. The court held that smartphones or tablets comply with this definition and can, therefore, be searched.

The court held in the Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others,

Zuma and Another v. the National Director of Public Prosecutions and Others (2008) case that it is a requirement in a South African environment that “premises” should be clearly defined. The question is then raised that if off-site searches of computers are permitted, what premises should be specified in warrants? Traditionally, premises are where suspects are located, but the presence of computers turns the search and seizure process around: the seizure of computers take place on a scene but the search of data takes place at the premises of forensic investigators. Should the premises of suspects be listed or the premises of forensic investigators or computers as premises? The answer was provided by the court during the Minister of Safety and Security v. Bennett (2007) case where the seizing of physical documents − prior to the search of these documents off-site − was permitted without a description of the secondary premises of forensic investigators. In the unreported judgment of the then Transvaal Provincial Division of the High Court, case 10828/2005 dated 13 May 2005, the court also expressed the opinion that it is irrelevant where forensic duplicates are created after seizure and removal from the scene.

Another issue is raised in this regard − if forensic investigators are planning to seize data on another network or at an online location, do the search and seizure warrants need to state the physical location from where forensic investigators are accessing the data or the physical location of where data is kept? (Kerr, 2005b:104). At the time when Kerr studied these aspects in 2005, cloud hosting was not as prevalent as it is today. If forensic investigators need to seize the files of persons kept in a virtual environment − hosted in a cloud − what premises need to be described? Search and seizure is further complicated by the structure of cloud hosting where one document can be broken up in a number of segments and each segment can be stored on a different server in a different country. The implications if this issue on search and seizure are recognised by the Australian Crimes Act (12 of 1914) Section 3LB and the New Zealand Search and Surveillance Act (24 of 2012), Section 111 – both these Acts permit law enforcement to search remote locations, such as online data storage facilities with no physical addresses nor a specific singular location, such as cloud services or where physical locations are unknown.

For the purpose of this study, the interpretation of “premises” is limited to the traditional description of premises or locations and not extended to describing devices as separate premises or the premises of digital forensic investigators.

3.1.5 Defining articles or items

The definition of articles or items should be sufficiently broad and flexible enough to accommodate forensic investigators to effectively search and seize within a digital context due to the nature of digital evidence and the magnitude of forms or file types and types of devices

evidence can be stored on or processed with. Bouwer (2014:171) observes that the Criminal Procedure Act (51 of 1977) is lacking in specifically including data as articles and stated that the legislature has recognised this omission by referencing the definition of articles and premises in the Electronic Communication and Transaction Act (25 of 2002), which states that data messages are classified as articles if these messages relate to a Section 20 article as defined by the Criminal Procedure Act (51 of 1977). Basdeo (2012b:198, 205) states that data refers to information that has been transformed into digital form and in terms of the provisions made in Section 20 of the Criminal Procedure Act (51 of 1977), which stipulates that anything can be seized and that anything should be susceptible to a wide enough interpretation to include data. Notwithstanding, Basdeo further advises that the provisions made in the Criminal Procedure Act (51 of 1977) should be restructured to alleviate the restrictive interpretation that articles are only physical items. Basdeo further expresses the opinion that law enforcement is currently interpreting articles very widely and they apply this definition to the seizure of digital evidence − a practise that has not yet been contested in court. This aspect is addressed in the Cybercrimes and Cybersecurity Bill which defines an "article" as any data, computer devices, computer networks, databases, critical databases, electronic communication networks or national critical information infrastructures or any part thereof or any other information, instruments, devices or equipment (Cybercrimes & Cybersecurity Bill, 2016:6).

For the purpose of this study, the interpretation of “articles” or “items” as per the proposed Cybercrimes and Cybersecurity Bill, is supported to include data, data storage devices and data processing devices.

3.2 Defining data and data messages

Article 1(b) of the Budapest Convention (Council of Europe, 2001a:4) defines computer data as any representation of facts, information or concepts in a form suitable for being processed on computers. The SALRC states that the definition provided by the Electronic Communication and Transaction Act (25 of 2002) of “data” and “data messages” is based on Article 2 of the United Nations Commission on International Trade Law’s (UNCITRAL) Law on Electronic Commerce with Guide to Enactment (1996) which use “data” and “data message” instead of the terms “electronic evidence” or “digital evidence” (SALRC, 2010:32). This approach is also recommended by the Practical Guide (SAPS, 2016:7) of the SAPS to use the description of “data” instead of “digital evidence”. To accurately make use of terminology in search and seizure warrants in line with enabling legislation, is supported in the case of Heaney v. S (2016) where the ruling was that the description of a suspected crime should be accurately described in line with enabling legislation and colloquially used terms should not be applied. The Electronic Communication and Transaction Act (25 of 2002) describes “data” as the electronic

representation of information in any form and “data messages” as data generated, sent, received or stored by electronic means. The SALRC further explains that in Part 2 of the UNCITRAL Model Law on Electronic Commerce (1996), it is stated that the concept of data messages is not intended to be limited to communication but should include computer records and all types of messages that are generated, stored or communicated in a paperless form (SALRC, 2010:32).

For the purpose of this study, the definition of “data” is viewed as an adaptation from Section 1 of the Electronic Communication and Transaction Act (25 of 2002) as the digital representation of information in any form and not the “electronic representation of data in any form”.

3.3 Digital, computer, electronic or cyber evidence

The SALRC observed that Article 2 of the UNCITRAL Model Law on Electronic Commerce (1996) refers to “data” and “data messages” rather than “electronic evidence” or “digital evidence” (SALRC, 2010:32). The reason for this is obvious since the Model Law on Electronic Commerce (1996), which forms the basis of the South African Electronic Communication and Transaction Act (25 of 2002), is aimed at regulating e-commerce and only a small portion of it relates to defining criminal activities. The UNCITRAL Model Law on Electronic Commerce (1996) stipulates that the law applies to all commercial activities (United Nations, 1996:3). It is, therefore, logical to rather use descriptions like “data” or “data messages”. Data or data messages become relevant during investigations into criminal activities, and then “electronic evidence” or “digital evidence” should be used. Bouwer (2014:170) recommends that a single definition for “electronic evidence” should be adopted in the South African law as “information of probative value stored or transmitted in digital format”.

During the research done for this study, it was found that various descriptions are used to describe concepts of digital, electronic, computer or cyber evidence. This is also applicable to digital crime, electronic crime, computer crime and cybercrime. It was found that in most instances, these terms are interchangeable and that most people know what is meant by these terms. It was, however, perceived that an understanding of these terms was relevant for legal correctness.

References to “computer” evidence or “computer” crime seem to be out-dated (Bouwer, 2014:161). The UNCITRAL Model Law on Electronic Commerce (1996) and the Electronic Communication and Transaction Act (25 of 2002) make reference to data, data messages and information systems instead of “computer”. The word “computer” is well-understood and is derived from what devices do, namely computing (Woodford, 2007). Computers are defined as “electronic devices which are capable of receiving information (data) in a particular form and of

performing a sequence of operations in accordance with a predetermined but variable set of procedural instructions (program) to produce a result in the form of information or signals" (Oxford Dictionary, 2016). This definition differs vastly from cellular phones with computing capabilities, but is described by the *Oxford Dictionary* as primarily a telephone connected via a cellular network over a wide area (Oxford Dictionary, 2016).

The term "cyber" is also of importance. In 1984, William Gibson originally coined the term "cyberspace" in his science fiction novel "Neuromancer" (Gibson, 1984). The *Oxford Dictionary* defines "cyber" as "relating to or characteristic of the culture of computers, information technology, and virtual reality" (Oxford Dictionary, 2016). However, this is not a very apt description from a legal point of view if one considers all the descriptions in which "cyber" is used, such as cyber bullying, cyberspace, cyber terrorism, cybersex. The use of "cyber" has become synonymous with the Internet, which then excludes devices upon which digital evidence can be located.

It is very difficult to differentiate between "electronic" and "digital". The SALRC shed light on this dilemma (SALRC, 2010:31). The commission states that while these two terminologies are used interchangeably, an important distinction exists between the two − analogue and digital outputs. Examples of analogue outputs are vinyl records, photographic films and old telephone systems making use of switchboards (Christensson, 2005). Neither the Electronic Communication and Transaction Act (25 of 2002) nor the UNCITRAL Model Law on Electronic Commerce (1996) provide any description or definition for "electronic". Spencer (2014) states that the term "electronic" is not particularly technical and has become synonymous with consumer electronics, such as clocks, radios, smartphones and tablets. It is, therefore, obvious that although "electronic devices" should include "data", it is not exclusively limited to "data". However, "digital" is based on binary coding and functions as the building blocks of data (Lowe, n.d). The Scientific Working Group on Digital Evidence (hereafter referred to as SWGDE) supports this by defining "digital evidence" as evidence stored or transmitted in a binary form (SWDGE, 2012:6).

For the purpose of this study, the term "digital" is used as opposed to the terms "electronic", "cyber" or "computer".

3.4 Forensic duplicating processes in relation to originality

Digital forensic investigations often involve creating and examining forensic duplicates of data under analysis (ACPO, 1997:4). Forensic investigators use forensic duplication techniques to collect or acquire data from hard drives as opposed to the normal copying of files. This is due to the fact that forensic duplicates contain all of the data from the source drive − even deleted files

(Nieman, 2006:44). A normal copying process only retrieves the active or currently accessible files, not deleted files as well (Kerr, 2005a:540). A number of references were found for the concept of creating forensic duplicates of digital evidence, including copies, clones, bit-stream copies, images, forensic copies, bit-by-bit copies, mirror images and acquisitions. Vandeven (2014:32-35) provides the following definitions for some of these concepts:

- *Bit-by-bit* or *bit-stream copies* − exact copies of all the bits of a logical volume or a physical drive. If the copies are made to files, it is referred to as forensic image files. If copies are made to another disk, it is referred to as clones or mirror images. The original and clones are identical and interchangeable, but if clones are not write-protected, subsequent actions of an analysis can alter the data.

- *Disk image files* − files containing exact copies of logical volumes or physical disks.

- *Forensic images* − exact copies of all the bits of logical volumes or physical drives that have been copied bit-by-bit and include all data and metadata. Forensic images include information, such as when these images were copied, by whom, with which forensic tools and the cryptographic hash used for verification of these images.

- *Raw images* − exact bit-by-bit copies of disks into a single file. Raw images do not contain information regarding the creation of these images.

According to Gerber (cited in Kessler, 2010:37), forensic duplicates were traditionally also referred to as “mirror” images, but because it confused courts, the use of “mirror” images are not recommended. Normally, mirror images are reverse images of originals.

All of these different terminologies can be confusing, but nowhere was it found in research that any of the terminology used − except “mirror copies” − is rejected by courts.

With newer technology becoming continually available while constraints are added, such as the sizes of datasets, digital forensic investigators are often required to forensically duplicate data selectively. In this sense, single files can be forensically duplicated or folders or partitions as opposed to a whole hard drive. Complete bit-by-bit duplicates of whole hard drives are, therefore, not always necessary.

In light of the above a single expression could prove to be technically incorrect in all situations. Whatever terminology is used, Lidbury and Boland (2012:1) state that what makes “collections” forensically sound should be the main aim − whether data was collected is an exact duplicate of the original source, including metadata. This implies that the collection method and subsequent analysis steps should not alter data and should include mechanisms to ensure the integrity of

data, such as the extraction of hash values. The judicial measures within a South African environment are the requirements specified by Section 14 of the Electronic Communication and Transaction Act (25 of 2002) − the originality of data messages are measured against the integrity of digital evidence from the time the data was first generated. Integrity is assessed by considering whether the evidence has remained complete and unaltered except for the adding of endorsements or changes, which is caused in the normal course of communication. Vacca (2005:795) states that an important feature of digital forensics is the fact that it changes the legal best evidence concept in digital evidence. Vacca states that a new concept of representational accuracy has emerged in terms of digital evidence − it is not necessary anymore to present original copies. If forensic duplicates are created and the source data is depicted exactly, duplicates are considered original (Vacca, 2005:237).

In the Canadian case of R. v. Munshi (2002), it was stated that with the modernisation of technology, forensic duplication processes have developed to such an extent that duplicate originals can exist. Although this ruling related to documents, the court stated that where exact replication processes are used, it is generally not necessary to compare original documents with duplicate originals.

Van Deusen Phillips (2010) maintains that the test of establishing if digital documents can stand as evidence, is to determine or prove that the content of documents is indeed the original, unchanged content. Van Deusen Phillips further states that this is normally accomplished by presenting original documents or duplicate originals. In the American case of Lorraine v. Markel American Ins. Co. (2007), the court held that an original is the writing itself or a counterpart intended to have the same effect and that if data is stored on computers or on similar devices, any printouts or other outputs readable by sight reflect the data accurately, the data can be accepted as original. In the case of Muller v. BOE Bank Ltd and Others (2010), it was acknowledged that South African courts have accepted and are accustomed to the creation or existence of “copies” recognised as duplicate originals since the inception of carbon copies.

For the purpose of this study, the most elucidating description, which should make room for interpretation, is the creation of “forensically-sound duplicate original records”. For ease of reference in this study, “forensic duplicates” is used.

3.5 Summary

The technical analysis and interpretation of terminology in relation to digital evidence are aspects that will be debated at length in South African courts in years to come. These interpretations can be problematic in terms of data, but a sound understanding can be gained from case law with regard to technical issues. In this chapter, the interpretation of concepts and

terminology was considered. It is argued that “premises” described in search and seizure warrants should be the premises of suspects and the interpretation of “search” should include actions in which the content of data becomes exposed. It is proposed that “search actions”, such as look, locate, separation of information, interpretation and analysis, should be recognised. The creation of forensically-sound duplicate original records should constitute the seizure of data as items or articles of digital information in any form and should be recognised as original duplicates.

In the next chapter, the international guidelines and standards guiding the digital forensic fraternity are reviewed.

CHAPTER 4 – DIGITAL FORENSICS AND INTERNATIONAL STANDARDS

4. INTRODUCTION

In the early 1900s, Dr Edmond Locard developed one of the cornerstones of modern-day forensic science, the Locard's exchange principle (Forensic Library, 2010). Locard, a French criminalist, was renowned for being a pioneer in forensic science and criminology. Whilst studying medicine, Locard developed an interest in the application of science to legal matters (The Forensic Library, 2010). Locard theorised that every time a person or an object comes into contact with another, it results in an exchange of physical materials. Locard believed that during this contact, all sorts of evidence, including human DNA, fingerprints, footprints, hair, skin cells, blood, bodily fluids, pieces of clothing, fibres and more are exchanged (Forensic Handbook, 2012). In 1997, Silvernail (1997:176-177) already stated that when persons start to use a computer, evidence of activities is created. It is, therefore, recognised that the Locard principle also applies to computers (Chisum & Turvey, 2000:11) due to evidential traces or artefacts exchanged between the network of victims and the computers of perpetrators. This is also confirmed by Wang (2007:8), who emphasises the fact that digital evidence can prove crucial links between victims and perpetrators.

If, as earlier discussed, it is recognised that computers have become an attractive medium for criminals (SALRC, 2010:7) and that their activities on computers result in evidence that can be linked to crimes of suspects (Casey, 2000:1, 6), it is essential to recognise the need for a discipline in the field of digital forensics.

Digital evidence is often collected incorrectly and analysed ineffectively or simply overlooked due to the complexities which digital evidence pose to forensic investigators (Casey, 2011:8; Craiger & Shenoi, 2007:49). This "new" type of evidence has prompted the beginning of a "new" type of forensic science − digital forensics (Kerr, 2005b:86). As with any forensic science, specific regulations, guidelines, principles or procedures should be followed to meet the objectives of investigations − the accuracy and acceptance of findings (Vacca, 2005:6). In this chapter, these regulations, guidelines, principles or procedures are discussed in the context of digital forensics: what processes should be followed and how these processes ensure the acceptability of digital evidence. These processes include international principles, such as the Association of Chiefs of Police Officers (hereafter referred to as the ACPO), and internationals standards, such as the International Organisation of Standardisation.

In this chapter, a summary is provided of the most influential or best-recognised international standards on digital forensics.

4.1 Digital forensics

Many definitions exist for digital forensics. Palmer (2001:16) captures the main aspects as the use of scientific derived and proven methods in locating, collecting, preserving, analysing, interpreting, documenting and presenting digital evidence relating to incidents, often with the aim of presenting evidence during hearings. The goal of the process is to preserve evidence in its most original form while performing a structured analysis by collecting, identifying and validating digital information for the purpose of reconstructing past events.

As a scientific-based discipline, digital forensics is premised on following set standards or methodologies in the above-defined processes, which are susceptible to inspection by judiciaries (Casey, 2011:10).

4.2 International standards

Nieman (2009:22) states that it is ironic that digital forensics first and foremost concerns forensic procedure, rules of evidence, legal concepts, precedents and processes and second to this, computers. It is exactly because of this, that standards in this field play such an important role.

However, it was found that very few absolute standards exist internationally to standardise the processes and procedures to be followed during digital forensic investigations. This is mainly due to the ever-changing information and communication technology environment and differences in local and international legislation relating to investigation methodology, rules of evidence and court procedures. The majority of “standards” are compiled as guidelines as opposed to set standards (International Organisation of Standardisation, 2014:vi).

In light of the importance of standards or the important role standards should play in digital forensics as a science, it is surprising that there are no set standards, rules or a protocol for the handling of digital evidence and that technical processes applied to digital evidence “do not have to pass any formal test” for digital evidence to be placed before courts (Scholtz, 2009:60). It is, therefore, understandable that the digital forensic industry has largely been self-regulated within a framework of international advised practices, case law, guidelines and industry groups.

4.2.1 Principles of the Association of Chief of Police Officers

The Good Practice Guide for Computer-Based Electronic Evidence (1997) of the ACPO was drafted in 1997. According to Mohay *et al*. (2003:123), these principles were reviewed during an International Hi-Tech Crime and Forensic Conference in October 1999 and were further formalised and accepted in 2001 at the 13th International Criminal Organisation's (Interpol) Forensic Science Symposium.

Digital evidence should be accurate, authentic and admissible like any other evidence and should conform to common law and legislative principles (Nieman, 2009:19). If investigators, for example, open files and make copies, move, save or print these files, these actions are not viewed as neutral and influence or modify evidence (Vacca, 2005:19). The Explanatory Report to the Cybercrime Convention indicates that digital evidence should be retained in the state it was found from the start to the point of prosecution (Council of Europe, 2001b:38). Kessler (2010:6) highlights the fact that each stage should be performed in such a way that the integrity of evidence is preserved.

The ACPO principles have long been a guideline for digital forensic investigators in formulating digital forensic procedures to ensure that the requirement as listed above are met when evidence is collected, handled and managed. The guide contains the following four principles concerning the collection and management of digital evidence (Association of Chief of Police Officers, 1997:4):

- *Principle 1*: No actions taken by investigators should change the data which may subsequently be relied upon in court.
- *Principle 2*: Only in exceptional situations should investigators work with or access the original data and only if they are competent to do so and in a position to provide evidence explaining the relevance and the implications of their actions.
- *Principle 3*: All processes applied to the digital evidence by investigators should be fully recorded to enable independent third party experts to follow these processes and reach the same results.
- *Principle 4*: Investigators should ensure that all legal principles are adhered to during the analysis of digital evidence.

The principles provide guidelines so that the actions of investigators do not change the digital evidence under investigation and if original evidence is accessed, it should be done by competent persons. A complete audit trail should be maintained so that the actions of

investigators can be reviewed, assessed and evaluated against local legal requirements. These international principles were drafted with the aim of ensuring that the handling of digital evidence conforms to the requirements of evidence in terms of the law and especially to ensure that the integrity of evidence is maintained by ensuring that data have remained unaltered (Association of Chief of Police Officers, 1997:6-7). The SALRC (2010:7) affirmed the importance of these principles when the commission stated that by accessing files, the actions of forensic investigators are not neutral and it is not easy to prove the integrity of digital evidence given the volatile nature of digital evidence. It was also stated that the incorrect following of crime scene protocols and proper procedures can render digital evidence unusable or vulnerable to claims of prejudicial distortion by the defence.

In chapter five, it is described how the Electronic Communication and Transaction Act (25 of 2002) of South Africa conforms to these requirements.

4.2.2 Standards and guidelines of the International Organisation of Standardisation

4.2.2.1 ISO 27037 − Security Techniques − Guidelines for identification, collection, acquisition and preservation of digital evidence

In October 2012, the ISO 27037 Standard on Information Technology − Security Techniques − guidelines for the identification, collection, acquisition and preservation of digital evidence was approved and published. The ISO standards are very well-known, but even the ISO standards seems to shy away from setting rigid standards in a digital forensic environment. In the opening line of the scope of the ISO/IEC DIS 27037 Standard (International Organisation on Standardisation,2012:1), it is stated that it merely provides “guidelines for specific activities in handling potential digital evidence; these processes are: identification, collection, acquisition and preservation of potential digital evidence”.

The processes specified in the standard set guidelines to ensure that digital forensic investigators maintain the integrity of digital evidence during the collection phases of investigations by following analysis methodologies aimed at advancing the admissibility of evidence during legal processes. The importance of the integrity of evidence is supported by Kanellis (2006:58) who emphasises that evidence should be managed correctly so that it cannot lose value and as a result, be inadmissible in courts. The ISO/IEC DIS 27037 Standard sets forth four fundamental principles for procedures to be followed in collecting digital evidence (International Organisation of Standardisation, 2012:8). Digital forensic investigators should:

- Minimise the handling of original evidence.

- Document all actions taken and account for any alterations in the data to allow experts to express an opinion regarding the reliability of the data.

- Adhere to local rules of evidence.

- Not take any actions beyond their competence.

The ISO/IEC DIS 27037 Standard specifies that in most jurisdictions, digital evidence is governed by three primary principles (International Organisation of Standardisation, 2012:6):

- Relevance

  A standard requirement is that only relevant data should be collected. In other words, the data collected should assist in examining incidents or aspects of incidents at hand and there should be a need and a reason to collect the data. This requirement is supported by Section 28, 31 and 210 of the Criminal Procedure Act (51 of 1977), which regulate wrongful searches and seizures, the inadmissibility of irrelevant evidence and the return of articles not required for criminal proceedings. Digital forensic investigators should be in a position to explain the procedures followed and validate the reasons and grounds why specific data was collected. Francoeur (2003:3) explains that the admissibility of any evidence should have an adequate level of relevance to the matter investigated.

- Reliability

  All processes followed in handling digital evidence should be auditable and repeatable. The result of applying these processes should be reproducible by independent parties when they follow the same process. Hofman (2006b:7) highlights that digital evidence should satisfy ordinary requirements related to the admissibility of documents. Documents should be authentic, reliable and original.

- Sufficiency

  Digital forensic investigators should ensure that all relevant information is collected to ensure that the matter at hand can be sufficiently analysed and considered. Digital forensic investigators should be able to provide an indication of how much data was considered and justify what was the basis on deciding what data and how much data to acquire.

The ISO/IEC DIS 27037 Standard specifies that all processes in relation to digital forensic processes should be (International Organisation of Standardisation, 2012:7):

- Auditable

  All processes, procedures and results should be auditable by independent forensic investigators to evaluate the activities performed by digital forensic investigators. Audits can be facilitated if the processes and actions followed by digital forensic investigators are sufficiently documented. Digital forensic investigators should be able to explain the basis upon which decisions were taken on what methodology was followed during analyses.

- Repeatability

  Repeatability is established when the same results are obtained in the following situations:

  - When the same procedures and methods are used.
  - When the same equipment under the same conditions are used.

  It should be noted that repeatability is not possible in all situations, for example when live data was analysed or volatile memory. In this case, digital forensic investigators should ensure that acquisition processes are reliable.

- Reproducibility

  Reproducibility is established when the same test results are produced under the following conditions:

  - When the same method is used.
  - When different equipment are used under different conditions.
  - When the same results can be reproduced at any time after the original test.

- Justifiability

  Digital forensic investigators should be able to validate all actions and methods used in identifying, collecting, analysing and managing potential digital evidence. Justification can be achieved by demonstrating that their decisions were best practice in a specific case in obtaining all of the potential digital evidence in existing circumstances.

In terms of handling digital evidence, the ISO/IEC DIS 27037 Standard advises that “devices that may contain potential digital evidence are removed from their original location to a laboratory or another controlled environment for later acquisition and analysis” and that forensic duplicates should be made for analyses to take place (International Organisation of Standardisation, 2012:9).

The standard sets out a number of phases during digital forensic investigations (International Organisation of Standardisation, 2012:8), which directly relate to searches and seizures, namely:

- *Identification* − includes the search for data storage devices, the recognition thereof and the documentation of processes followed. It also entails the prioritisation of the sequence of methods used to secure digital evidence, which can be volatile.

- *Collection* − relates to the collection and removal of evidence or the acquisition of evidence on a scene.

- *Acquisition* − entails the creation of forensic sound duplicates of evidence in the least restrictive manner possible.

- *Preserving evidence* − from the point of collection throughout all of the digital forensic processes followed.

The above-mentioned phases is normally achieved during the search and seizure actions of forensic investigators on a scene. These phases are described during the process of digital seizures and divided into two distinctly different stages, namely the search of physical devices on a scene and later searches for relevant data (Kerr 2005b:87). To ensure that evidence is not compromised, forensic duplicates are created of originals and forensic duplicates are analysed (Kessler, 2010:37). The process followed in creating forensic duplicates, should ultimately stand up to legal scrutiny (Nieman, 2009:22).

According to Nieman (2009:18), the ultimate goal is to ensure that evidence is admissible in a court of law and to preserve the evidential weight during the collection of digital evidence. The collection of digital evidence is a forensic and procedural process, which should always be performed with care (Kanellis, 2006:273). In the Explanatory Report to the Convention on Cybercrime, the complications of collecting digital evidence as opposed to tangible objects were considered and it was stated that digital evidence requires special rules in respect of collection and preservation. Data should be collected in such a way that the information is retained in the exact state it was found (Council of Europe, 2001b:33).

Nieman (2009:20) recalls that “in the early days” of digital forensics, digital evidence was copied as files or raw sectors. As newer technology and processes became available, methods were replaced with imaging or the acquisition of digital evidence. Cross (2008:210) explains that “acquisition” refers to the process of collecting digital evidence from specific devices, normally computers of suspects or victims.

A standard process is described that is relied on during subsequent discussions of searches and seizures for digital evidence due to the fact that the emphasis of this study was not on the technical detail of forensic imaging processes.

The process of creating forensic duplicates usually commences by removing the hard drive from the computer of victims or suspects and to connect the hard drive to a write-protector device (Nieman, 2009:22). This procedure is in line with the principles set out by the ACPO (1997:4) and the ISO (2012:6-8) − the actions of investigators should not change data and where possible, forensic duplicates should be made of the relevant data and these forensic duplicates should be analysed.

A write-protector device places a computer in a read-only form (US DOJ, 2004:41). This device prevents actions taken by investigators, such as opening and closing files, searching through files or influencing or changing metadata. This device allows digital forensic investigators to conduct preliminary searches on computers to establish if these computers contain relevant information or not. A write-protector device can also be a software program, which can be used to prevent changes being made to the information stored on computers. A good analogy is a piece of glass laid over a letter. Any potential changes due to actions of investigators cannot be transferred to the evidence, just as changes made with a highlighter on the glass is not transferred to the actual letter, but investigators are permitted to view and read the letter.

At this stage, evidence can be browsed to determine if it contains relevant evidence or if imaging can be started without browsing the evidence. Once it is determined that devices contain relevant evidence, forensic duplicates should be made of the evidence. This is done by means of a number of forensic software programs, which allow digital forensic investigators to create forensic duplicates of devices. Nieman (2009:22) explains that bit-by-bit copies do exactly what the name suggests – copies are created bit-by-bit. A bit is the smallest size data can be broken up into, an exact replica of every sector of a hard drive. Bit-by-bit copies are exact reproductions of digital records that contain all of the data, even hidden or deleted data (Angermeier, 2010:1615). Forensic duplicates and original pieces of evidence are exact copies of each other based and proven on scientific principles and they can, therefore, be considered as duplicate originals (Van Deusen Phillips, 2010). With current technology available, digital forensic investigators are able to collect a single file from a computer or a whole folder or the whole hard drive, including empty or unallocated space (Vandeven, 2014:1). Collections can be done without deviating from forensic requirements. To create forensic duplicates, can be a lengthy process. According to the Digital Intelligence (Digital Intelligence, 2016), an average transfer rate to create forensic duplicates, is approximately 6GB per minute. If a hard drive is 500GB in size, it takes, therefore, 83 minutes to create one forensic duplicate and another 83 minutes to verify the integrity of a forensic duplicate. Creating forensic duplicates of a server

can easily take more than 12 to 24 hours. The implications of multiple computers and servers on a scene can have a great impact on the duration of collection processes.

During collection processes, forensic programs use a cryptographic hashing algorithm to ascertain the hash value of data. This is referred to as the MD5 hash algorithm or SHA1 hash algorithm. Nieman (2009:22) correctly state that this hash value is often referred to as the electronic fingerprint of a piece of data.

The MD5 hash algorithm is a 128 bit hash value while the SHA1 algorithm is a 160 bit hash value and the SHA1 hash is considered to be a more complex and more secure algorithm (Thompson, 2005:39). Schneier (1996:436-441) explains that the MD5 hash value has a key size of 128 bits with 3.4 × 1038 possible combinations. The chance of randomly finding two files that produce the same hash value should be computationally unfeasible. Digital forensic investigators can, therefore, mathematically − beyond a reasonable doubt − show in court that digital evidence has not changed by even one character.

This hash value is the way in which digital forensic investigators can, mathematically, beyond a reasonable doubt, show in court that the digital evidence has not changed by even one character.

An example of hash values for the word “CAT” is:

MD5 hash value - c01ae1a5f122f25ce5675f86028b536a

SHA1 hash value - cf9b775c2c444520178d30c267440066c6eff6e8

Losey (2007) explains that if one single character in a computer is changed, the hash value changes. If the word “CAT” is changed, for example, to “CATS”, the hash values change to:

MD5 hash value - ee77f71f2b809c0f6d92320fc9b480f6

SHA1 hash value - c7da99899675795b2f1d94607dbe57b731dd2255

Brown (2010:28) states that an imaging process is a scientific process and subject to the Daubert reliability test (Kessler 2010:4), which was formulated in Daubert v. Merrell Dow Pharmaceuticals, Inc. (1993). This scientific requirement is further discussed in the ISO/IEC DIS 27043 Standard below.

4.2.2.2 ISO/IEC 27043 Standard on Information Technology − Security techniques − Incident investigation principles and processes

The American Academy of Forensic Sciences identified digital forensics as a forensic science (American Academy of Forensic Sciences, 2008). As a scientific discipline, digital forensics should meet the same standards as other scientific and technical evidence to be admissible in court (Kessler 2010:20). The final draft of the ISO/IEC 27043 Standard on information technology − Security techniques − Incident investigation principles and processes (International Organisation of Standardisation, 2014:4) specify that persons can be considered experts based on their experience, knowledge, skill, training or education. The opinions, theories, processes, procedures and tools used by experts should be evaluated against the Daubert test (Daubert v. Merrell Dow Pharmaceuticals, Inc, 1993), which has for long been the *defacto* test in the United States of America and is applied by courts to scientific procedures used to prepare or uncover evidence. The Daubert test comprises of the following factors that should be taken into account to ensure the integrity of evidence (Daubert v. Merrell Dow Pharmaceuticals, Inc, 1993):

- The theories and techniques used by experts should have been tested.
- The theories and techniques should have been subjected to peer review and should appear in publications.
- Any error rates should be known to the experts and have been reported.
- Experts should be governed by standards governing their applications.
- The theories and techniques used by experts should enjoy widespread acceptance.

The ISO/IEC 27043 Standard expanded and sets out the different phases of a digital investigation. It is divided into two main areas, namely digital investigation processes and concurrent or parallel processes depicted below (International Organisation of Standardisation, 2014).

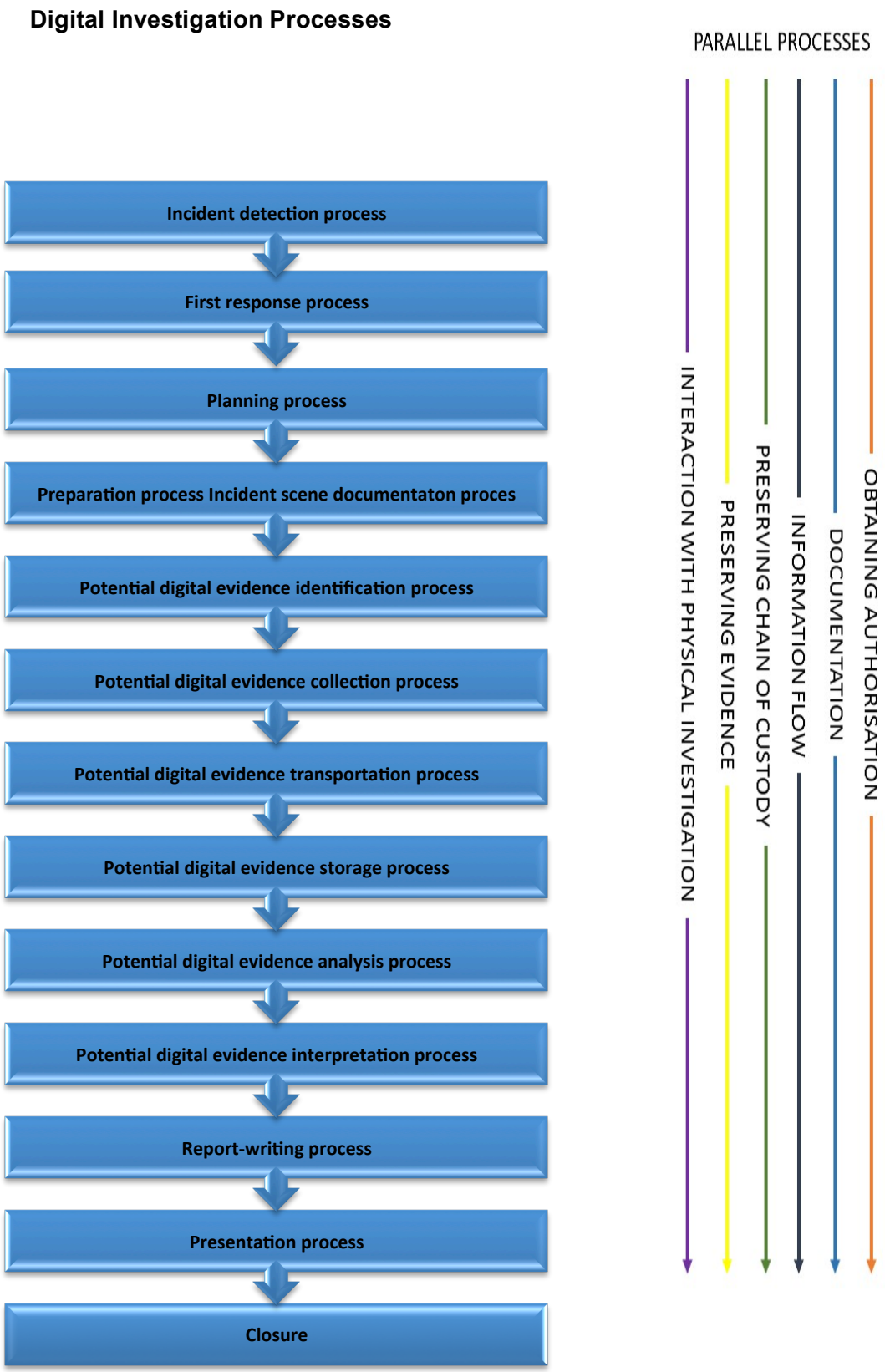

Figure 2 – Digital forensic processes (International Organisation of Standardisation, 2014:14)

A summary of the different phases of a forensic investigation (International Organisation of Standardisation, 2014:14-21), as depicted in Figure 2 include:

- *Detection phase* – incidents are detected.
- *First responder phase* − digital forensic investigators attend to incidents.
- *Planning phase* − investigations of incidents are planned.
- *Preparation phase and scene documentation phase* − preparation steps are taken to investigate incidents and document actions are taken on scenes.
- *Evidence identification phase* − potentially relevant evidence is identified.
- *Evidence collection phase* − evidence is collected.
- *Evidence transportation phase* − evidence is transported from scenes to digital forensic laboratories.
- *Evidence storage phase* − digital evidence is securely stored.
- *Evidence analysis phase* − evidence is analysed to determine relevance.
- *Evidence interpretation phase* − evidence is interpreted in relation to its evidential value.
- *Reporting phase* − evidence is reported on.
- *Presentation phase* − testimonies or overviews are provided regarding evidence.
- *Closure phase* – cases are archived.

The parallel processes include:

- Obtaining of authorisation to investigate incidents.
- Documentation of all actions during investigations.
- Continual information flow between digital forensic investigators and forensic investigators.
- Maintaining chain-of-custody.
- Preserving the integrity of evidence.

- Interaction with physical investigations.

A number of the parallel processes set out by the standard were of paramount importance to this study:

Obtaining authorisation

Proper authorisation should be obtained for each process performed during an investigation. Authorisation may be required from government authorities, system owners, system custodians and principals. For the purpose of this study, proper authorisation is achieved by the application for search and seizure warrants in terms of the provisions stipulated in Section 20 or 21 of the Criminal Procedure Act (51 of 1977).

Preserving the chain of custody

A traditional requirement for proving the integrity of evidence is the chain of custody. Van der Merwe *et al.* (2008:85) state that the prosecution needs to convince the court that the evidence was not interfered with from the time it was seized to the presentation in court. It is, therefore, critical that forensic investigators should ensure that digital evidence remains secure throughout the analysis (Cross, 2008:211).

A chain of custody requirements were expanded upon in the ISO/IEC DIS 27037 Standard and these requirements relate to the ability of digital forensic investigators to account for all the acquired evidence from the point when it was within their custody (International Organisation of Standardisation, 2012:10). A chain of custody can be viewed as a record that chronologically captures the movements and handling of evidence. A chain of study should contain:

- A unique identifier.
- Who accessed the evidence at what time and place.
- Who checked the evidence in or out of storage and for what reason or under whose authority.
- Any unavoidable changes made to the evidence, who made changes and a justification for introducing the evidence to court.

Schetina *et al.* (2002:351) together with Lange and Nimsger (2004:76) state the importance of a chain of custody in relation to the admissibility of digital evidence and that courts need to be informed concerning the measures that were adhered to. A chain of custody ensures that

evidence was not tampered with. Digital forensic processes − if followed and executed correctly − support and contribute to the chain of custody requirements.

4.3 Summary

In summary, the originality, reliability, integrity and admissibility of digital evidence should be maintained as follows:

- Data should not be changed or altered.
- Forensic sound duplicates should be created.
- Digital forensic analyses should be performed by competent persons.
- Digital forensic analyses should adhere to relevant local legal requirements.
- Audit trails should exist consisting of all required documents.
- Chains of custody should be protected.
- Processes and procedures should be proper while recognised and accepted by the industry.
- When possible, forensic duplicates should be made of evidence.
- Original evidence should not be directly examined.

If the ACPO (1997) principles and ISO/IEC 27043 and 27037 Standards are followed as a forensic framework, then digital forensic investigators should follow these standards as a legal framework. In the next chapter, a legal framework is discussed with regard to how these principles are enforced or supported by international and local legislation.

CHAPTER 5 − LEGAL FRAMEWORK

5. INTRODUCTION

Digital forensics and the legal system are inseparable life partners. US-Cert (2005:1) defines this relationship as "... the discipline that combines elements of the law and computer science to collect and analyse data from computer systems, networks, wireless communications and storage devices in a way that makes it admissible as evidence in a court of law".

Digital evidence is intangible − one never knows what lies below the surface until it is exposed to examination or how reliably the evidence was handled by digital forensic investigators until an examination during testimony. Nieman (2009:22-23) states that digital forensics is one of the most intimidating occupations in the information technology field − every aspect of the technical competency and methodology used by digital forensic investigators is scrutinised to its very core. It is, therefore, imperative that digital forensic investigators follow clear procedures during analysis processes.

The ultimate goal of digital forensic analyses is to establish reliable facts. If the evidence is questioned, it should withstand scrutiny − most often scrutiny in judicial processes. If the evidence fails the scrutiny of judicial processes, all of the efforts up to that point are wasted. No purpose is served by being the best digital forensic investigator in the world and you are unable to apply the regulations that govern the discipline. Casey (2011:23) states that each segment in a digital forensic process should be performed to maintain the integrity of the evidence and to ensure its admissibility.

In the Lorraine v. Markel American Ins. Co. (2007) case, it was stated that the legal threshold is an important preliminary standard to test evidence, but it is subject to later scrutiny by cross-examinations. Cole *et al.* (2015:96) mention that digital forensic investigators are often called to court with regard to the integrity of digital evidence, but the threshold pertaining to the reliability and authenticity of digital evidence is currently not high. It can be argued that this is due to a lack of knowledge concerning digital evidence, procedures or legal requirements. In the case of S v. Ndiki (2008), the court held that digital evidence should be submitted in South African courts as real or documentary evidence and that the relevant rules of evidence should be applied accordingly.

The measurement of the integrity of digital evidence is done via the requirements of the regulatory framework. In this chapter, these aspects are discussed and what the legal threshold for digital evidence is. The development of local and international regulations, treaties and

conventions is discussed and these requirements with regard to the search and seizure of digital evidence are reviewed.

This study was performed from an investigative perspective and not from a legal perspective.

5.1 The Budapest Convention on cybercrimes

South Africa was a signatory state to the Cybercrime Convention in Budapest in 2001. The Budapest Convention is an international agreement aimed at addressing cybercrime globally by harmonising national legislation, improving investigative methodologies and improving cooperation amongst countries (Nieman, 2006:101). As a signatory of the Budapest Convention and in terms of the provisions of Section 39(1)(b) of the Constitution (1996), South Africa needs to comply and/or take cognisance of the procedural provisions of the Budapest Convention (Basdeo, 2012b:196).

The Budapest Convention and its Explanatory Report was adopted on 8 November 2001. It was submitted for signature in Budapest on 23 November 2001. South Africa is one of the original signatory states, but has not ratified this report yet (Couzyn *et al.* n.d.).

The Budapest Convention recognises that cybercrime should be addressed as a priority by adopting appropriate legislation and international cooperation (Council of Europe, 2001a:2). The convention cautioned that the proper balance between the interest of law enforcement and the respect for fundamental human rights should be ensured.

While the Budapest Convention set specific requirements for criminal law, it provided very generic descriptions of procedural law and left it to local legislation to further define these descriptions − no more so than what South Africa already has in legislation, such as the Criminal Procedure Act (51 of 1977). Section 19 of the Budapest Convention relates to the adoption of legislation, which empowers competent authorities to (Council of Europe, 2001a:11-12):

- Seize or secure computer systems or storage mediums.
- Make and retain duplicates of computer data.
- Maintain the integrity of stored computer data.
- Remove seized data.

However, these guidelines do not provide guidance in a South African context in terms of current complications that digital evidence pose to legislation. The application of “pre-digital era”

viewpoints, terminology and doctrine are still applied with regard to digital evidence (Kerr, 2005a:533). Section 19 of the Budapest Convention specifies that domestic search and seizure mechanisms of digital evidence should be equivalent to the power of the searching for and seizing of tangible articles (Council of Europe, 2001a:11-12). Article 19 of the Budapest Convention provides for the search and seizure of data, but does not recognise data as tangible objects susceptible to search and seizure. Seizures normally focus on the medium on which data is saved or stored (Council of Europe, 2001a:11-12). Basdeo (2012b:211) further confirms that this type of national legislation is required to provide local law enforcement with mechanisms to assist other countries.

The Explanatory Report to the Convention on Cybercrime requires that the power of search and seizure and violations of constitutional rights should be proportional to the nature and circumstance of offences, judicial oversights should be taken into consideration and the rights of third parties should be respected (Council of Europe, 2001b:24). This report also recognises the fact that there is a need for existing legislation to be updated and legislation should be brought in line with new terminology that better encapsulates concepts of digital evidence (Council of Europe, 2001b:33).

5.2 The Constitution of the Republic of South Africa

Search and seizure or inspection mandates are captured in criminal legislation, civil legislation and regulations. The power of each differs substantially, but all need to adhere to the Constitution (1996). As the supreme law, the Constitution (1996) ultimately dictates how searches for and seizures of evidence may be performed in South Africa. Chapter 2 of the Constitution (1996), which is also referred to as the Bill of Rights, embodies the basic rights of all people in South Africa − including the right to dignity and privacy. The courts play a major role in ensuring that the obligations imposed by the Constitution (1996) are fulfilled by applying fair law and interpretations of constitutional rights are vigorously and justly entrenched in case law (Basdeo 2009:4). It is, therefore, only fitting to start this chapter by looking at fundamental constitutional rights and the limitations of these rights as set out by the Constitution (1996).

The Bill of Rights stipulate that everyone is equal before the law and everyone has an equal right to protection or to be benefited by the law. Every person has a right to dignity and the right to have their dignity respected and protected (Constitution, 1996). The SALRC explains that through an indirect application of the Bill of Rights, all regulations are subject to and should be given content in light of the basic values of the Bill of Rights (South African Law Reform Commission, 2005:5). In Section 39(2) of the Constitution (1996), which relates to the interpretation of the Bill of Rights, a court, tribunal or forum should (1) promote the value that

underlie an open and democratic society based on human dignity, equality and freedom; (2) should consider international law; and (3) may consider foreign law. In this regard, courts have an obligation to develop common law in accordance with the spirit, objects and purports of the Bill of Rights. The spirit, objects and purports of the Constitution (1996) were expressed by the court in the case of Shabalala v. the Attorney-General of Transvaal (1995) as:

> *The aspiration of the future is based on what is "justifiable in an open and democratic society based on freedom and equality". It is premised on a legal culture of accountability and transparency.*

Basdeo (2009:2) remarks that in the dispensation of the Constitution (1996), the right to privacy from government intrusions with regard to citizens, their property and possessions, has become an expectation from South Africans. Section 14 of the Constitution (1996) specifically applies in relation to searches and seizures and sets out the right to privacy of persons − their home, person or property may not be searched or seized or the privacy of their communications infringed upon.

The right to privacy is deeply rooted in history. Psychological and anthropological evidence suggests that even in the most primitive societies, measures are adopted to allow individuals privacy (South African Law Reform Commission, 2005:3).

In the case of Investigating Directorate: Serious Economic Offences v. Hyundai Motor Distributors (Pty) Ltd v. Smit (2000), the court referred to Section 14 of the Constitution (1996) as the "right to privacy in the social capacities in which we act". The right to privacy is not qualified by "personal" and the word "private" is not used in a 1996 Constitutional context. This allows for a much wider interpretation of "privacy". It is argued that this interpretation can, therefore, extend the perception of privacy to areas, such as online storage areas for data or closed online discussion groups.

The right to privacy is generally well-understood and well-defined. Basdeo (2012a:164) argues that pre-trial procedures or search and seizure procedures constitute an important consideration in relation to the Bill of Rights − while it is conceded that law enforcement officers have the right and have special powers to investigate crime, such powers can inevitably result in the violation of rights and freedoms of individuals. It is for this reason that Section 36 of the Constitution (1996) − also known as the Limitation Clause − sets out limitations to these rights and states, therefore, that the Bill of Rights can be limited by means of a law of general application, given that the limitation is reasonable and justifiable based on dignity, equality and freedom and by taking into account all relevant factors, such as:

- the nature of the right;

- the importance of the purpose of the limitation;
- the nature and extent of the limitation;
- the relation between the limitation and its purpose; and
- less restrictive means to achieve the purpose."

The SAPS are empowered by Section 205(3) of the Constitution (1996) to "prevent, combat and investigate crime, to maintain public order, to protect and secure the inhabitants of the Republic and their property, and to uphold and enforce the law". Section 13(1) of the South African Police Service Act (68 of 1995) specifies that subject to the Constitution (1996), members of the SAPS may only exercise their functions with due regard to the fundamental rights of persons and Section 13(4) of the South African Police Service Act (68 of 1995) declares that members shall be competent to execute any warrant directed to them or to any other SAPS member (South African Police Service Act, 1995).

Section 36 of the Constitution (1996) makes, therefore, allowance for investigative organisations, such as the SAPS, to conduct searches and seizures in terms of authorizing legislation in the form of the Criminal Procedure Act (51 of 1977). The Criminal Procedure Act is a law of general application, but it also recognises that the State should not be permitted untrammelled access to search and seize property of individuals. It is a necessity of democracy that individuals should be protected against unjustified actions of the State (Basdeo, 2009:1). This limitation, as discussed above, is normally effected when search and seizure warrants are obtained. By obtaining search and seizure warrants, the issue is highlighted whether the necessity these warrants overrides the right to privacy of individuals (Basdeo, 2009:14).

What is important from the limitation in Section 36 of the Constitution (1996), is the statement that the least restrictive means should be followed to achieve a specific purpose. It is, therefore, is understood that while Section 36 of the Constitution (1996) allows law enforcement to conduct search and seizure operations, these operations should be conducted in such a manner that the least restrictive means to achieve a specific purpose, is followed. This further highlights the question as to whether computers containing data can be searched or forensically duplicated.

Section 35(5) of the Constitution (1996) stipulates that evidence obtained in a manner that violates any right listed in the Bill of Rights, must be excluded if such evidence renders trials unfair or acts detrimental to the administration of justice. Unconstitutionally-obtained evidence is not always inadmissible in courts, but only if this evidence (1) renders trials unfair; or (2) is otherwise detrimental to the administration of justice. In the case of Powell NO and Others v.

Van der Merwe and Others (2004), the court held that evidence is only rendered inadmissible if the disallowing of the unconstitutionally-obtained evidence is a vindication of the right that was violated and prevents the infringer from benefiting from the infringement.

Lowenstein (2007:4) is of the opinion that the constitutional right of individuals is heightened due to the seizure of computers and all that they contain by the State. The seizure of computers can be viewed as very intrusive since people tend to keep vast amounts of private and confidential information on their computers. Casey (2011:1) also refers to this issue and states that in a digital age, the constitutional rights of individuals are especially important due to the level of privacy, which is associated with digital devices in relation to communication and the extensive nature of information stored on these devices (Guzzi, 2012:302).

5.3 The Criminal Procedure Act, 51 of 1977

According to Basdeo (2009:138), the Criminal Procedure Act (51 of 1977) has long been the primary statute under which the SAPS have the right to conduct searches and seizures in South Africa − with or without warrants. These rights are not left entirely to the discretion of the SAPS, but are subject to authorisation of authorised officers.

Section 21 of the Criminal Procedure Act (51 of 1977) sanctions authorised officers to issue search and seizure warrants authorising police officers to enter premises and to search premises and persons on the premises to find and seize specific items on such premises − if there are reasonable grounds to believe that articles involved in the commission of a crime will be found on the premises. These articles, which may be seized according to Section 20 of the Criminal Procedure Act (51 of 1977), are limited to articles, which is believed or on reasonable grounds believed to be (1) involved in the commission of a crime; (2) can be used as evidence; or (3) intended in the commission of a crime.

It is such a short, seemingly straightforward and simple paragraph, yet it has far-reaching implications, which have been fiercely fought over in many courts across South Africa. As was expressed in the case of NDPP and Another v. Mohamed (2003), the search and seizure of articles from a premises is a significant invasion upon the rights of individuals and should be completed within clearly defined limits so as to impact as little as possible on the rights of affected individuals.

When the Criminal Procedure Act (51 of 1977) is compared with the Budapest Convention or similar legislation from the United Kingdom (British Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners, 2013), American Federal Rules of Criminal Procedure, (2009), Australian Crimes Act (12 of 1914) and the New Zealand Search

and Surveillance Act (24 of 2012), it is noticed that no provision is made for referencing digital evidence and remote search and seizures.

When measuring the Criminal Procedure Act (51 of 1977) against Section 19 of the Budapest Convention, the wording of Section 21 of the Criminal Procedure Act (51 of 1977) fails to address issues. Courts provide purposeful interpretations to these Sections, but disputes during interpretations can be caused with regard to the following issues:

- No general authorisation is extended to searches and seizures at remote locations.
- No authorisation is provided for the off-site continuation of searches for data and no guidance on the extension of search and seizure warrants throughout processes is provided.
- No specific authorisation is provided for the search and seizure of data to:
    - seize or similarly secure digital evidence.
    - make and retain forensic duplicates of digital evidence.
    - render data inaccessible or remove digital evidence.
- No specific powers are available to order any third party to assist the SAPS with securing or accessing digital evidence.
- No provision is made for private digital forensic investigators to assist the SAPS with searches and seizures for digital evidence.

The proposed Cybercrimes and Cybersecurity Bill − if approved − will address some of these issues. Nieman (2009:427), Basdeo (2012b:198, 205) and Bouwer (2014:170-171) recommend that the Criminal Procedure Act (51 of 1977) should be amended to include and recognise specific aspects of digital evidence. An inclusion can prevent similar arguments, which resulted in the recent verdict in the case of the Minister of Police and Others v. Kunjana (2016) where the Constitutional Court ruled that the seizure of articles under Section 11(1)(a) and (g) of the Drugs and Drug Trafficking Act (140 of 1992) without a search and seizure warrant was unconstitutional since the SAPS have less restrictive mechanisms available in terms of the provisions of Section 21 and 22 of the Criminal Procedure Act (51 of 1977).

5.4 The Electronic Communication and Transaction Act (25 of 2002)

The statutory requirements of digital evidence in South African courts are set out in the Electronic Communication and Transaction Act (25 of 2002), which is based on the UNCITRAL

Model Law on Electronic Commerce (1996) of the United Nations Commission on International Trade Law adopted in 1996 (South African Law Reform Commission, 2010:29). The UNCITRAL Model Law on Electronic Commerce (1996) is supplied as a model law to all member territories. As a member state, South Africa has enacted the Electronic Communication and Transaction Act (25 of 2002) based on the UNCITRAL Model Law on Electronic Commerce (1996) (South African Law Reform Commission, 2010:29).

Although the Electronic Communication and Transaction Act (25 of 2002) does not relate directly to the search and seizure of digital evidence − except for Section 80 to 84 of the Act, which sets out the authority of cyber inspectors in relation to searches and seizures − it sets requirements for digital evidence in relation to originality, admissibility, integrity and reliability.

Some of the most relevant statutory requirements for the authenticity and admissibility of digital evidence are set out in Section 14 and 15 of the Electronic Communication and Transaction Act (25 of 2002). The importance of these two sections in relation to the search and seizure of digital evidence relates to the fact that during searches and seizures the originality, integrity and reliability of evidence should be maintained. In other words, the actions of police officials on a scene and their subsequent interactions with digital evidence can have a direct impact on the acceptance of evidence in court procedures. Nieman (2009:19) comments on the fact that digital evidence differs drastically from other types of evidence and that the very process of collecting digital evidence can change this evidence in significant ways.

Section 14 and 15 of the Electronic Communication and Transaction Act (25 of 2002) provide requirements for the measurement of digital evidence − normal aspects of the rules of evidence or the subsequent evaluation thereof are not excluded. Section 14 of the Electronic Communication and Transaction Act (25 of 2002) relates to the originality of data messages and stipulates that where the law requires information to be presented or retained in its original form, requirements should be met if the integrity of digital evidence − from the time it was first generated to its final form − has passed assessment. The integrity of digital evidence is assessed by considering whether the evidence has remained complete and unaltered except for the addition of endorsements or any changes, which can be caused in the normal course of communication, storage or display.

A discussion of Section 14 of the Electronic Communication and Transaction Act (25 of 2002) is required since it was determined that this issue has so far not been addressed by any court case in South Africa. What is meant by the “original form” and “final form” of information? Does the “original form” of data messages indicate the first time when a subject, for example, originally typed a document and is the “final form” the final version of the document when a subject last worked on the document? Or is the time when the evidence is presented in court in

its “final form” or does the “original form” relate to when the evidence is presented as a forensic duplicate in court or should this be viewed as the “final form”? This discussion is important since it is believed that legislators do not consider the implication that the originality of evidence should be assessed at a point prior to where the data is considered as evidence, nor can it mean that the original form is the same after a forensic duplicate is created. A logical conclusion is that an “original form” is the format of the data on computers of suspects when the forensic investigators arrive on a scene and that the final form is the form in which evidence is presented in a court.

Section 15 of the Electronic Communication and Transaction Act (25 of 2002) relates to the admissibility and evidential weight of data messages and states that the rules of evidence should not be applied so as to deny the admissibility of data messages on the grounds that these messages are in the form of data messages. This Act also stipulates that in assessing the evidential weight of data messages, the reliability of the manner in which the data messages were generated, stored or communicated and the reliability of the manner in which the integrity of data messages should be maintained. The period in which these assessments of reliability takes place should be specified. It is argued that it is logical that the intention of legislators is that the reliability of data should be assessed from the point where data is collected by the forensic investigators or seized from suspects to the point where data is presented in a court.

Section 14 and 15 of the Electronic Communication and Transaction Act (25 of 2002), therefore, support the ACPO principles (Association of Chief of Police Officers, 1997:4) and the ISO Standards (International Organisation of Standardisation, 27043 and 27037) − no actions performed by investigators should change evidence and maintaining the reliability of evidence is of the utmost importance. From these Sections, it can be concluded that South African courts test the integrity of digital evidence by assessing whether evidence was changed by the actions of analyses and reliability is tested by assessing the methods used in collecting and processing digital evidence. Judges play an important gatekeeper role in determining if scientific evidence can be accepted in their courts and just as judges need to eliminate junk science from court cases, they also need to keep out digital evidence of poor quality (Kessler, 2010:6, 100).

Section 80 of the Electronic Communication and Transaction Act (25 of 2002) makes provision for the appointment of cyber inspectors who can with the authority of warrants (Section 82(1)) enter premises that have bearing on investigations and they may search these premises with the aim of seizing articles (Basdeo, 2012b:206). Section 81(2) of the Electronic Communication and Transaction Act (25 of 2002) state that any statutory body with powers of inspection or powers of searches and seizures in terms of any law − specifically referring to the SAPS − can apply for assistance from cyber inspectors. Basdeo (2012b:206) maintains that the reason for these requirements are not apparent and that when cyber inspectors are approached, they

should do so in an advisory capacity and without taking over investigations. From Section 81(1) of the Electronic Communication and Transaction Act (25 of 2002), which provides for the general powers of cyber inspectors, it seems clear that cyber inspectors should report any unlawful activities to appropriate authorities and that it is not the intention of legislators to replace police members with cyber inspectors. Nieman (2006:17) is of the opinion that the SAPS cannot utilise the procedural provisions of the Electronic Communication and Transaction Act (25 of 2002) without the assistance of cyber inspectors.

5.5 Proposed Cybercrimes and Cybersecurity Bill

The Proposed Cybercrimes and Cybersecurity Bill (2016) is currently in a consultation document format to receive comments made by the public and should be introduced to Parliament during the last quarter of 2016. The aim of the Cybercrimes and Cybersecurity Bill is to combine all of the aspects relating to cybercrime and to bring it under one "umbrella Act". Section 20 of the Cybercrimes and Cybersecurity Bill places a requirement on Cabinet members responsible for consulting with the National Director of Public Prosecution and other Cabinet members responsible for the administration and issuing of standing operating procedures to the SAPS when investigating offences in relation to crimes in terms of the Cybercrimes and Cybersecurity Bill (Cybercrimes & Cybersecurity Bill, 2016:25).

The Cybercrimes and Cybersecurity Bill (2016:6) provides for a wider definition of "access" and "articles". This definition allows for the duplication of data − forensic duplicates – and that data is viewed as objects. Another very valuable proposition in the Cybercrimes and Cybersecurity Bill (2016:8) is the definition of "inspector" which is widened to include persons who are not law enforcement officers, but who are appointed by the National Commissioner of the SAPS due to their expertise to assist law enforcement officers in relation to digital forensics as specified by Section 28 of the Cybercrimes and Cybersecurity Bill. Inspectors cannot be empowered without the presence of law enforcement officers present. The presence of inspectors can alleviate constraints as identified in the case of Smit and Maritz Attorneys and Another v. Lourens No and Others (2002), where the court ruled that private persons cannot not assist the SAPS on scenes with searching for and the seizing of digital evidence.

The Cybercrimes and Cybersecurity Bill also provides a definition of "computer", "computer data storage device" and "computer system" as opposed to just providing a definition for "information system" as currently stated in the Electronic Communication and Transaction Act (25 of 2002). The Practical Guide of the SAPS (2016:16, 20) refers police officials to the Electronic Communication and Transaction Act (25 of 2002) that provides a definition of "information system" as "information system means a system for generating, sending, receiving, storing,

displaying or otherwise processing data messages and include the Internet" and adds the following interpretation: "An information system would therefore include articles commonly referred to as a computer, cellular telephone, flash drive, "USB" device, compact disk and digital photograph and or video disc or card". The SAPS Interim Standing Operating Procedures Dealing with Electronic Evidence (SAPS, 2016:3) refers more inclusively to "electronic devices" and the definition includes devices, such as computers, data storage devices, cellular phones, smart cards, answering machines, scanners, digital cameras and global positioning systems, which can be the source of digital evidence.

Section 23(2)(d) of the Cybercrimes and Cybersecurity Bill allows for the search of data or computer devices while Section 29(2)(e) and (f) of the Cybercrimes and Cybersecurity Bill allows for the search and seizure of data by duplicating data as specified in search and seizure warrants (Cybercrimes & Cybersecurity Bill, 2016:25). These two Sections make the following reference: "to the extent as is set out in the warrant". This reference can be interpreted to mean that the description of data should be specified in search and seizure warrants or it can also be interpreted to mean that the extent of forensic duplications should be specified in search and seizure warrants.

Section 24 of the Cybercrimes and Cybersecurity Bill makes provision for oral applications of search and seizure warrants for digital evidence (Cybercrimes & Cybersecurity Bill, 2016:25). Oral applications of search and seizure warrants should be transcribed within 48 hours.

An area not addressed in these above-mentioned Acts, is the search of remote locations, such as online data storage facilities with no physical address nor specific singular locations, such as cloud services or where physical locations are unknown, as specified by the Australian Crimes Act (12 of 1914) Section 3LB and the New Zealand Search and Surveillance Act (24 of 2012), Section 111, which both allow law enforcement to search these locations.

5.6 Summary

Basdeo (2009:30) states that search and seizure in terms of the provisions made in the Criminal Procedure Act (51 of 1977) is most probably the most complicated area in criminal procedure. Search and seizure encompasses detailed legal provisions and faces a variety of complications. Basdeo further maintains that due to overlapping between the Bill of Rights and the Criminal Procedure Act (51 of 1977), search and seizure often requires vigorous examination to determine if the Constitution (1996) has been violated. In this section, legal requirements were reviewed that form the foundation for the next chapter to understand the implications of technical complications that digital evidence poses to a legal framework.

CHAPTER 6 – TECHNICAL AND DOCTRINAL IMPEDIMENTS

6. INTRODUCTION

It is clear from cases, such as the U.S. v. Comprehensive Drug Testing Inc. (2009) and the Canadian case of R. v. Vu (2013), that other countries are grappling with similar complexities in relation to potential complications that digital evidence pose to local legislation. The United States of America has a vast amount of documented cases, especially in terms of the Fourth Amendment of their Constitution (hereafter referred to as the Fourth Amendment), which protects citizens against unreasonable search and seizure procedures (Legal Information Institute, n.d.).

Lowenstein (2007:6) purports that traditionally search and seizures have developed with physical locations in mind. These processes with regard to physical locations have had the benefit of being honed and improved by court cases over many years as opposed to digital evidence, which is relatively new. A proper balance between law enforcement and the privacy rights of individuals will be the focus point in future digital cases. Courts will focus on digital complexities, which over time will result in a clear understanding and interpretation of these impediments (Chan, 2014:458).

It is very difficult to determine where South Africa is with regard to understanding and interpreting these impediments − if not in the beginning phase − and how prior experiences in other countries, such as Canada, the United Kingdom, Australia and the United States of America can aid South Africa due to the fact that so few cases and aspects have been tested in South African courts. It is, therefore, important to review perceived impediments which digital evidence pose to the law to fully understand how these impediments can have an impact on the South African legal framework and how these complexities can be approached in a South African context.

In this chapter, a summary is provided of perceived international impediments that digital evidence pose to search and seizures. International and local authoritative cases are reviewed that identify specific issues or doctrinal impediments to search and seizure procedures in general or search and seizure procedures for digital evidence specifically. These impediments are discussed and considered individually, although a level of overlapping exists due to the close proximity of aspects between areas, in more detail in subsequent sections. South African case law is not discussed separately, but is integrated into the discussion of international case law of each impediment.

6.1 Overview of international doctrinal impediments

Kerr (2005b:100-108) investigated a number of complexities that search and seizure procedures with regard to digital evidence pose to traditional laws. Kerr listed the following areas as doctrinal difficulties relating to aspects that should be considered when compiling and authorising search and seizure warrants:

- How should the articles, to be seized, be described and is data really seized if the forensic duplicate is the article which is seized as opposed to the original device? – If search and seizure warrants only describe computer equipment, these warrants can be considered too broad if the computer and all the data on it is seized − if warrants only describe the data, the seizure of the physical computers can be viewed as unconstitutional.

- When does the law regard a computer "searched" and what is the premises to be searched? – If search and seizure warrants describe the premises of suspects, is the removal of computer equipment to digital forensic laboratories by law enforcement officers permissible to continue searching the data?

- When can searches be executed – If the computer equipment is seized from the premises of the suspect, strictly speaking, the search and seizure warrant has been executed and the subsequent search of the data at a later point may not be covered by the original search and seizure warrant?

- What are the oversight and record keeping requirements? – This relates to the documentation of how the digital forensic investigator will stay inside the search and seizure warrant with the analysis and does the accused have a right to oversee that this search is performed inside these parameters. Also once the relevant information is found, what record is supplied to the suspect in relation to which articles or documents have been seized.

Additional technical complications were argued and considered in the landmark case of the United States v. Comprehensive Drug Testing Inc. (2009), which spanned from 2002 to 2009. It is important to review aspects of this case to fully understand the implications, consequences and arguments with regard to the above-mentioned impediments.

In 2002, the government of the United States of America obtained a search and seizure warrant to seize the records of ten baseball players who were suspected of drug use. The search and seizure warrant included the provision to seize computer records from a company called Comprehensive Drug Testing Inc. and to search and segregate data off-site. To justify the off-

site search of data, the application to the search and seizure warrant set out the difficulties and hazards of collecting digital evidence, including the acknowledgement that computers containing all of the data will be seized and that information beyond the scope of the search and seizure warrant will be seized. Based on this application, the judge granted what is called a "broad" seizure, but also included some restrictions, such as that non-investigating law enforcement officers should segregate the related and non-related data instead of case agents. The objective of the segregation restriction was that case agents could not access information outside of the scope of the search and seizure warrant. During the search of computers at the premises of Comprehensive Drug Testing Inc., a directory or folder named "Tracey" was located, which contained all the names of all of the major league baseball players who tested positive for steroids. The investigators decided that it was impractical to sift through the evidence on the scene and removed the data off-site. The case agents ignored the segregation restriction in the search and seizure warrant and took possession of all of the data directly. Based on the information from the "Tracey" directory, the State obtained additional search and seizure warrants for the information regarding the data of additional players that were identified. The State based this on the fact that the information was discovered in plain view.

Comprehensive Drug Testing Inc. and the association of the players appealed this seizure. The U.S. v. Comprehensive Drug Testing Inc. (2009) case spanned multiple jurisdictions and two courts ordered the return of the data. The judges expressed grave dissatisfaction with the State's conduct and labelled their conduct as manipulation and misrepresentation. The State appealed these two decisions to the Ninth Circuit Court, which reversed the two court's orders to return the data to the players.

In August 2009, the case was then taken before a full bench of judges (hereafter referred to as *en banc*) who reversed the decision and instructed that all testing results, except that of the original ten baseball players, be returned to the players. The panel reviewed the conduct of the State and reflected on the balance between law enforcement's, perhaps legitimate need in relation to digital evidence to over seize, and the restrictions against overbroad searches. After studying this, the court directed authorised officers to enforce the following pre-emptive requirements (hereafter referred to as *ex ante* requirements):

- The State must waive reliance on the plain view doctrine. If investigators find anything on computers that does not relate to the original search and seizure warrant, they are not allowed to use or access this information.

- Segregation of relevant and non-relevant data must be either done by specialised personnel or an independent third party.

- If segregation is done by the State, it must be agreed on in the search and seizure warrant application that computer personnel may not disclose to the investigators any information other than that which is the target of the warrant.

- Search and seizure warrant applications must state the actual risks of the destruction of information and prior efforts to obtain the information by means of other legal routes.

- The search protocol of the State must be structured to only uncover information containing probable cause, and only that information may be examined by investigators.

- The State must destroy or return non-related data.

These requirements sparked various discussions and legal battles. Guzzi (2012:329) reported that the ruling has been criticised as an impractical, costly and overbroad solution. In September 2010, the Ninth Circuit Court issued a revised *en banc* opinion and changed the above-listed requirements to guidelines.

It should be noted that in the Matter of the United States of America's Application for a Search Warrant to Seize Electronic Devices from Edward Cunnius (2011:12), the court stated that although the requirements concerning the case of U.S. v. Comprehensive Drug Testing Inc. (2009) were changed to guidelines, it does not mean that judges are prohibited from using or insisting on the State to comply with the ruling or that the guidelines are inappropriate. A very interesting approach by the court in this case was to state that there was no suggestion that the use of independent filter teams or a waiver of the plain view doctrine would compromise the State's ability to successfully prosecute cases. Independent filter teams are teams or individuals who are not connected with an investigation directly and their function is to sift through data and determine what is relevant and what not or what is privileged and what is not (US Department of Justice, 2009:110-111). During an unstructured interview (Anon, 2016b) with an advocate working with investigations concerning the Competition Act (89 of 1998), it was established that the Competition Commission of South Africa has extensively adopted this approach over the past few years when conducting investigations. The interviewee (Anon, 2016b) stated that the Competition Commission makes use of external consultants for digital forensic investigations. These external service providers are responsible for creating full system forensic duplicates of all devices on a scene and independently retain the sealed evidence. After search and seizure procedures have been completed, the Competition Commission enters into a tripartite agreement or contract with respondents and the digital forensic service providers on how electronic discovery processes will be managed in relation to the analysis of the data. The

Competition Commission provides external service providers with keywords that are used to locate relevant data. These keywords are not disclosed to respondents to prevent them from gaining insight into investigations. After the segregation of potentially relevant information and non-relevant data, the data is then given to respondents by the external service providers to identify legally privileged information. Following this, only potentially relevant data – and no legally privileged data – are handed to the investigators of the Competition Commission for further investigation by the external service providers. The identified legally privileged data can be verified by an external third party.

In the U.S. v. Comprehensive Drug Testing Inc. (2009) case, the court warned that if rules are so relaxed to accommodate complications posed by digital evidence, there is a serious risk that every search and seizure warrant for digital evidence would become overbroad and that the Fourth Amendment becomes irrelevant. This situation also applies to the South African Constitution (1996) if acceptable legal parameters of search and seizure warrants for digital evidence are not defined.

6.2 Search and seizure warrants in South Africa

In the Gaertner and Others v. the Minister of Finance and Others (2013) case, the court explained that “Kubomvu” (meaning red or danger in Zulu) is a warning traditionally given by a lookout when the SAPS enter a township area in South Africa. This word is also synonymous with “run away”. The power of the SAPS to search persons and the premises of persons in the apartheid era in South Africa is one of the main aspects that caused mistrust, hatred and fear in communities. These emotions were not unfounded since this power was often mercilessly, severely and blatantly misused. Memories of these injustices are still evident from many comments and references made in judgements of the Constitutional Court relating to search and seizure by the SAPS, such as the court’s remark in the case of Magajane v. the Chairperson of the North West Gambling Board (2006) that “our history provides much evidence for the need to adhere strictly to the warrant requirements”.

South Africa − just like many other democratic countries worldwide − require by means of a search and seizure warrant process, that the State show under oath, before a neutral authorised officer, why sufficient grounds exists to warrant the breach of a suspect’s rights. In the Minister for Safety and Security v. Van Der Merwe and Others (2011) case, it was stated that search and seizure warrants govern the time, place and scope of intrusions or violations.

Obtaining search and seizure warrants under the Criminal Procedure Act (51 of 1977) was identified by the court in the Magajane v. the Chairperson of the North West Gambling Board (2006) case as a tried and tested mechanism whereby courts can defend individuals against the

power of the State and against unlawful searches. Search and seizure warrants issued in terms of the provisions stipulated in the Criminal Procedure Act (51 of 1977) are an important weapon that assists the SAPS in performing their constitutional mandate of preventing and investigating crime. However, by utilising this powerful tool, they interfere with the equally important rights of individuals. Safeguards are, therefore, needed to ameliorate the effect of these infringements by limiting the extent to which the rights of individuals are impaired.

The intrusive nature of search and seizure warrants and the obligation of the South African judicial system to guard against the misuse of this authority are well-documented in the case of Powell NO and Others v. Van der Merwe and Others (2004) when the court said the following:

> *Our law has a long history of authorized search warrants with rigor and exactitude – indeed, with sometimes technical rigor and exactitude. The common law rights so protected are now enshrined, subject to reasonable limitation, in s 14 of the Constitution and further that the general ransacking of a person's home has not been permitted since 1891.*

The court maintained that due to the danger of misuse in the execution of power in relation to the search and seizure of evidence, the court has an obligation to examine the validity of search and seizure warrants and their execution with "jealous regard for the liberty" of suspects.

The following requirements of search and seizure warrants were set out in the case of Powell NO and Others v. Van der Merwe and Others (2004):

- A court must scrutinise the validity of search and seizure warrants with jealous regard for the rights of suspects both in terms of the authority under which these warrants are issued and their ambit.
- The terms stipulated in search and seizure warrants must be construed with reasonable strictness.
- Search and seizure warrants must convey the authorised scope very clearly to both searchers and suspects.
- If search and seizure warrants are too general or the specified terms go beyond what were authorised by the statute, courts will not recognise these warrants as valid and they will be set aside.

In the Minister for Safety and Security v. Van Der Merwe and Others (2011) case, the court stated that aggrieved suspects can question the validity of search and seizure warrants on the basis that these warrants were too vague – overbroad − that it extend beyond what is permitted

by the statute or is absent of jurisdictional facts that are foundational to issuing the search and seizure warrant.

Overview of SAPS digital forensic processes

An unstructured interview was held with a former police officer who is an expert in digital forensics and the management of digital forensic units of the SAPS. An unstructured interview was necessary to establish what the current processes within the SAPS in relation to search and seizures for digital evidence are. This was necessary due to the fact that the procedures that the SAPS use are not available in the public domain. According to Anon (2016a), current processes within the SAPS concerning search and seizures for digital evidence are as follows:

- The SAPS have three capacities in the digital forensics field. One capacity is concerned with the collection of intelligence; the second is responsible for conducting digital forensic investigations for the broader units within the SAPS while the Directorate of Priority Crime Investigations (hereafter referred to as the DPCI) has its own capacity, which focuses on priority crimes.

- The SAPS has centralised digital forensic laboratories in inter-alia Pretoria, Johannesburg, Cape Town, Bloemfontein, East London and Durban.

- When drafting applications for search and seizure warrants, forensic investigators have access to members of their digital forensic laboratories, but assistance is only required when acceptable terminology is needed to describe the articles under investigation.

- The DPCI has a larger ratio between forensic investigators and digital forensic investigators than the units responsible for general digital forensic investigations in the larger SAPS due to the fact that the DPCI unit is smaller. Digital forensic investigators working for the DPCI are, therefore, able to attend to more than 80% of the unit's crime scenes. It is estimated that within the general SAPS, this percentage is very low and can be as low as 20%.

- There are no parameters set out in terms of retaining seized computers other that the provisions stipulated in the Criminal Procedure Act (51 of 1977). The DPCI is able to − after seizing cellular phones – to return these phones approximately within a week and computers within two weeks, but cases with larger quantities approximately within two months. In general, the rate of returning seized articles by the SAPS is closer to two months on average. The DPCI has created a triage team to expedite the turnaround time on investigating and returning cellular phones.

- The review of data by digital forensic investigators at the DPCI is normally conducted within 30 days, but investigations do not necessarily start immediately after a search and seizure. The average SAPS turnaround is between 60 to 90 days with some cases being up to 18 months.

- The assistance of digital forensic investigators is requested via an application form. This form is limited in specifying the date and time assistance is required.

- Digital forensic investigators are not supplied with copies of search and seizure warrants and normally only confirm whether their names appear on warrants.

- Instructions pertaining to what analysis functions are required from digital forensic investigators are done on a separate application for analysis form. On this form, investigating officers normally identify what type of information is required. Typical requests are to extract “all data generated or relating to users”; “all email communication” or specified keywords. On cellular phones, all of the content is generally copied and handed over to investigation officers.

- If reports are required, the reports are done in the form of statements, according to Section 213 of the Criminal Procedure Act (51 of 1977). In these reports, emphasis is limited to chain of custody aspects and the evidence found on devices. Very limited information is provided on the analysis methodology followed.

The interviewee expressed the following general opinions that do not directly relate to the processes followed by the SAPS when conducting search and seizures for digital evidence:

- The biggest problem concerning requests made by investigating officers in relation to the scope of the analysis, is the fact that they are not sufficiently trained and do not exactly know what they should be looking for. The interviewee is of the opinion that this uncertainty creates the impression that investigators are going on “fishing expeditions” and they hope to find some evidence by sifting through all of the data on computers or cellular phones.

- Concern was expressed regarding the fact that some units in the SAPS return the original devices to the suspect. The interviewee is of the opinion that original hard drives should be retained for court purposes and not the forensic duplicates.

6.3 A South African perspective on doctrinal impediments

The following doctrinal impediments were identified after studying international subject material:

- Should data or physical devices be described in the search and seizure warrant?
- Are off-site searches permitted?
- Should the State wave the plain view doctrine?
- Is the segregation of data a requirement?
- Is search and seizure the least restrictive manner of achieving the objectives?
- Should the State specify search protocols?
- Should the State return non-responsive data?

The question arose whether these aspects are issues and relevant in a South African legal environment. The study discovered no local cases where these aspects were scrutinised comprehensively, although the following corresponding or similar aspects were encountered which warrant further research.

6.3.1 Obligation to provide full disclosure with applications for search and seizure warrants

The Constitutional Court stated in the case of Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008) that applicants of applications brought to the court without the knowledge or presence of suspects, have a duty of good faith and should place all relevant material facts before authorised officers. This ruling was also supported by the Supreme Court of Appeals in the case of Powell NO and Others v. Van der Merwe and Others (2004) that applicants of search and seizure warrants are under duty to be ultra-scrupulous in disclosing facts that may influence authorised officers. The interpretation is that the Constitution (1996) requires judicial officers to read legislation in a way that gives effect to its fundamental values. It is acknowledged that search and seizure operations are vital in the fight against crime and that the State has an obligation to protect citizens against crime. This obligation is sufficiently important to justify breaches in the privacy of individuals. However, law enforcement officers are not permitted to invade the privacy rights of persons without good cause. In the Goqwana v. the Minister of Safety NO and Others (2016) case, the court expressed the opinion that search and seizure warrants should not be viewed as “mere interdepartmental” correspondences or “notes”. It is a substantive weapon in the arsenal of the State, it embodies awesome power with formidable consequences and must be issued with care after careful scrutiny.

When evaluating applications for search and seizure warrants, authorised officers should exercise their discretion to authorise search and seizure warrants in such a way that the rights of persons are protected as far as possible. After the authorised officer has taken the decision to approve the application for a search and seizure warrant the authorised officer should then ensure that the search and seizure warrant is not too general nor overbroad and that the terms are reasonably clear. If one considers the study performed by Kessler (2010) regarding the level of understanding and awareness amongst judges in the United States of America concerning digital evidence, it needs to be considered that a greater than usual explanation or description of what the forensic investigator is requesting regarding the search and seizure of digital evidence, should actually be a requirement. This is especially relevant if one considers that in the case of Smith, Tabata and Van Heerden v. the Minister of Law and Order (1989), it was held that if the articles have been described in broad and general terms, the court will rule that the authorised officer did not apply his mind properly. The question can then be asked if authorised officers do not have sufficient knowledge concerning the unique complexities which digital evidence pose to traditional search and seizure operations, can it then be concluded that they were in a position to apply their mind sufficiently. In light of the custodial or the constitutional protector's role that judges play in assessing whether sufficient grounds exist to permit a breach in the constitutional rights of persons and to ensure that a breach is done in the least restrictive manner, a certain level of knowledge is required or sufficient disclosure to place authorised officers in a position to apply their mind. This was the conclusion of the Supreme Court of Canada in the case of R. v. Vu (2013) when the court held that applications to search and seizure warrants must explicitly stipulate, and so also the warrants, that a search of a computer on a premises is required and authorised due to the unique complications which computers pose to a person's privacy. The court held that only then can the court be sure that authorised officers considered the full range of distinctive privacy concerns that computer searches raise, and having done so, the threshold has sufficiently been reached to permit infringements of the rights of persons.

In examples located locally, such as the case of Imperial Crown Trading 289 (Pty) Ltd v. Birch NO and Others (2012) in relation to applications for digital search and seizures warrants, it was found to only focus on laying the foundation why reasonable grounds exists to believe that the search and seizure is needed to further the investigation. One needs to consider the minority ruling in the Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. National Director of Public Prosecutions and Others (2008) case where it was stated that applicants of search and seizure warrants should disclose all of the facts that "might be" regarded as reasonable and relevant, because these facts can influence decisions of authorised officers. These officers cannot consider selected facts or an edited version of facts. Following the ruling in the Thint (Pty) Ltd v. the National Director of Public Prosecutions and

Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008) case, the question arose if the following aspects, as examples, should be mentioned in applications for search and seizure warrants for digital evidence since it could be material. These questions below need to be considered also in light of the ruling in the Canadian case of R. v. Vu (2013) where the court required that the mere fact that computers will be searched should explicitly be stated in applications to ensure that authorised officers can consider if enough grounds exist to breach the level of privacy that individuals have come to accept with computers, cellular phones and tablets. The following questions are addressed in subsequent sections:

- Should the application describe that computers containing all of the data − including non-relevant and potentially legal privileged documents – will be seized?
- Should the application describe that computers will be seized and that off-site searches will be conducted?
- Should the application indicate how long the computers will be removed before the equipment is returned to the owners and what impact these delays will have on the owner or a business?
- Should specific details of the analysis process and the search protocol be documented in the application, such as the keywords, what files will be accessed, what measures will be employed to stay within the ambit of the search and seizure warrants and , what measures will be taken to protect privileged data?

In support of these issues, it was established that the SAPS Interim Standing Operating Procedures Dealing with Electronic Evidence (SAPS, 2016:12) recognise, to a limited extent, these requirements and instruct investigators to specify both in applications and in search and seizure warrants whether forensic duplicates will be made on site or off-site. A further requirement, as highlighted in the U.S. v. Comprehensive Drug Testing, Inc. (2009) case, can be to explain to authorised officers what other avenues have been explored to achieve the same goal or as required by the Constitution (1996), if warrants are the least restrictive manner of achieving specified goals.

It was acknowledged by the court in the Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008) case that forensic investigators cannot be expected to disclose facts of which they were not aware at the time of submitting the applications for a search and seizure warrant for approval. Computers have become so prevalent in the commission of crimes that it should be a clear consideration, which the forensic investigator should make, based on his knowledge

concerning the investigation and the crime which was committed if a computer can be or was involved. It can be reasoned that if forensic investigators do not have a clear idea about what should be searched or seized, search and seizure operations can be viewed as mere “fishing expeditions”. In the case of Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008), the court expressed the opinion that applicants should be able to make decisions with regard to which facts can influence authorised officers. The court cautioned that the test of materiality should not be set so high that it makes it practically impossible for the State to comply with its duty of disclose or applications being so extensive that they overburden judicial officers. In the Minister of Safety and Security v. Bennett (2007) case, the court also pointed out that with applications for search and seizure warrants, the State only needs to show reasonable grounds to motivate the issuing of search and seizure warrants and not prove a *prima facia* case.

An aspect of caution to be kept in mind when applying for search and seizure warrants, is the recent ruling by the High Court in the Heaney v. S (2016) case where it was found that copies of search and seizure warrants and any documents these warrants refer to, such as the applications for warrants, should be handed over to suspects upon request. The court held that search and seizure warrants directly indicate that these warrants were issued based on “information under oath” and that applications for search and seizure warrants are, therefore, integrally linked to the validity of the issuance and execution of search and seizure warrants. The applications and the search and seizure warrants should, therefore, immediately be handed over to suspects upon request. The Court ruled that immediate handover can facilitate and expedite court applications by the suspects to protect their rights. This ruling is also in line with the constitutional rights of persons to have access to information “that is held by another and that is required for the exercise or protection of rights” − also supported by the Promotion of Access to Information Act (2 of 2000).

6.3.2 Search protocol and *ex ante* restrictions

There are two approaches that can be followed to limit the invasiveness of search and seizure warrants for digital evidence: pre-emptive restrictions (hereafter referred to as *ex ante* restrictions) and after-the-fact scrutiny (hereafter referred to as *ex post facto* scrutiny). The *ex ante* restrictions are imposed on search and seizure warrants prior to approval and execution. These restrictions set out the process to be followed by forensic investigators and what measures should be taken to limit invasiveness with regard to search and seizure warrants (Kerr, 2005a:566). In this approach, search and seizure warrants are regulated in terms of defining:

- How searches should be conducted and how access to files will be restricted to only relevant files − search protocol.

- Where searches are going to take place and for how long devices are going to be retained – these issues are discussed in subsequent sections.

The second approach, *ex post facto* scrutiny, is not to restrict search and seizure warrants, but to subject search and seizure warrants and the execution thereof to standards of review by the court after the fact, which is the general practice in South Africa.

Lowenstein (2007:13) states that most courts are rejecting *ex ante* restrictions. This was in 2007, before the U.S. v. Comprehensive Drug Testing, Inc. (2009) ruling where *ex ante* restrictions were first set as requirements and thereafter changed to guidelines. In the case of United States v. Vilar (2007), the court expressed the opinion that by specifying *ex ante* restrictions, authorised officers can place themselves in a position to tell the State how to run their investigations − something that authorised officers are not qualified to do. This issue was again raised by Guzzi (2012:305) who is of the opinion that due to the unpredictable nature of digital forensic scenes, it is overly impractical or too limiting to place *ex ante* restrictions on warrants. This opinion is in line with the court's comment in the case of Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008) − authorised officers should be vigilant and not hamper the State's ability to prosecute crime when the rights of suspects are protected.

Two aspects are relevant when considering *ex ante* restrictions. The first aspect is if authorised officers are authorised or in a position to place restrictions on forensic investigators *ex ante* and secondly, what restrictions are in the interest of justice. Guzzi (2012:305, 321) is of the opinion that it is impractical to have authorised officers impose restrictions who are not well-equipped to understand the implications of these restrictions or to review them. Guzzi maintains that it is "potentially technologically inappropriate" and can be potentially unlawful for authorised officers to impose restrictions.

A search protocol does not relate to the search methodology, which is followed when scenes are searched, but sets out in applications of search and seizure warrants how digital forensic investigators should search through the content of computers (Welty, 2011:9). Following a search protocol is not meant to determine the content of documents, but to determine if documents are relevant or a measure to determine which documents are irrelevant to an investigation (Guzzi, 2012:321).

In South Africa, authorised officers are found not to be in the practice of setting restrictions on warrants or requiring search protocols. In the Thint (Pty) Ltd v. the National Director of Public

Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008) case, the court reviewed the requirements of Section 29(5) of the National Prosecuting Act (32 of 1998). If the issuing of search and seizure warrants is considered, authorised officers should determine if there is a reasonable suspicion that an offence has been committed and that articles that have a bearing on an investigation, can be located on the premises. Only after this threshold has been met, should authorised officers consider the terms of search and seizure warrants. The court also expressed their view that the validity of warrants should be assessed by common law principles, but constitutional issues should also be taken into account and the spirit of the Bill of Rights. The court, in the case of the Minister for Safety and Security v. Van Der Merwe and Others (2011), expressed the opinion that safeguards are necessary to limit the effect that search and seizure warrants has on the rights of persons. The court highlighted that these safeguards, include specifying procedures for issuing warrants and should reduce the potential of abuse during their execution of warrants. Although the study did not find case law in which authorised officers set out *ex ante* requirements in South Africa, it is clear that it is the prerogative of authorised officers to reject applications for search and seizure warrants if they find applications wanting in areas. In the Canadian case of R. v. Vu (2013), the court expressed the opinion that they have a responsibility to not only evaluate if the constitutional rights of persons were violated *ex post facto*, but the court also has an obligation to protect these rights by considering the constitutional rights of persons when applications for warrants are considered *ex ante*.

Computer searches can be unusually intrusive and can reveal tremendous amounts of other information. Information stored on computers is so intermingled, that it is not possible to segregate information effectively on a scene or prior to seizure (Lowenstein, 2007:10). Even if information can be segregated, relevant system data is kept at various locations on computers and cannot be extracted as evidence unless the whole hard drive is forensically duplicated. Welty (2011:9) reported that due to the fact that digital evidence on computers is intermingled, forensic investigators should demonstrate how they plan on searching for relevant information to minimise an invasion of privacy. The South African Constitution, Section 36(1e) stipulates that the least restrictive means should be followed to achieve a specific purpose. In the case of the United States v. Mann (2010), it was emphasised that search and seizure warrants for obtaining digital evidence should be detailed and tailored to only allow access to files in question and to nothing more. Search protocols can involve a myriad of possibilities and can include a specification of keywords that will be searched, the types of files that will be accessed and can also be limited or specified. Metadata and hash values can be searched or other more sophisticated approaches or newer available technology can be applied, such as predictive coding, clustering, content analytics and auto-categorisation (Guzzi, 2012:319). Forensic investigators can utilise, for example, metadata searches to locate specific files authored by a

user or determine dates when documents were created, modified or accessed or they can use a hash library to locate, for example, child pornography without opening files. What needs to be considered in light of available technology, is that if regulations are so relaxed due to current constraints and if technology improves – are regulations going to be revisited and amended to be more restrictive or would the less restrictive measures have then become the norm?

Although it was stated in the case of the United States v. Mann (2010), that search and seizure warrants should be detailed and exact to only discover related files, this is easier said than done. The court held in the case of the United States v. Burgess (2009) that there may be no practical alternative to the State looking in many of the folders or files stored on a computer or in all of them. The court, however, held that in order to protect the rights of suspects, investigators should first look in the most obvious places and then – when necessary − progressively move from the obvious to the obscure. It was argued that by following search protocols, forensic investigators can demonstrate their intent to limit the invasiveness of search and seizure warrants.

Search protocols are susceptible to both *ex ante* and *ex post facto* judicial reviews. These protocols are, therefore, subject to more stringent evaluations or greater judicial reviews. Not only is the description of sought objects evaluated, but also the proposed methodology which will be followed in locating these articles and ultimately, the actions that were taken during the search. Many different views exist in favour or against search protocols. Based on these views, the balance between the privacy rights of suspects and the interest of law enforcement should swing in favour of law enforcement opposed to the protection of innocuous or merely private data (Guzzi, 2012:320). This opinion is strongly supported by the United States Department of Justice (2009:79-82) where the department warned that to place search parameters on analyses can seriously impair the State's ability to locate evidence and prosecutors should oppose these restrictions. One proposed restriction is to limit an analysis to a keyword search. Very few digital forensic investigations will be complete and accurate by only conducting a keyword search. Files are often scanned and these scanned files, or documents saved as pictures on a computer, are unresponsive to a keyword search. Suspects can also make use of encryption, passwords or code words. In the United States v. Hill (2006) case, it was found that the reasonableness of the investigator executing a seizure and performing a subsequent search remains subject to later judicial review. It is further advised by the United States Department of Justice (2009:82) that if search protocols are included in applications, it should be clearly stated that these protocols are illustrations of likely strategies to be followed and not a "specification of the exact manner that will be followed". In the United States v. Mann (2010) case, the proposition was made that a fully-fledged search protocol should still be used, but on a voluntary basis. Courts can, therefore, use agreed-upon protocols to restrict reasonable limits to

plain view discoveries. In this approach, all data that fall inside the original search criteria, are susceptible to plain view discoveries while other data is off limits. This can be the genesis of self-imposed regulations by forensic investigators that can go a far way in showing courts that balance was sought in the interest of justice by responsible and mature forensic investigators.

The Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners of the British Attorney General (2013:24-25) provide clear guidance that lead investigators should develop a strategy setting out how data should be analysed to identify certain categories of data. If forensic tools are used to sift through data, it is "usually appropriate" to provide suspects with a list of reasonable search terms. This process may be required to be repeated a number of times since searches may be conducted more than once. A detailed record should also accompany the strategy used and the analytical techniques used to search the data, should also be included. Records should include the names of the persons who carried out the process, what keywords were used and specify the dates and times of all actions.

In the Canadian Supreme Court case R. v. Vu (2013), it was argued that *ex ante* search protocols should be a requirement of all warrants and that search protocols were required to limit the scope of digital searches to ensure that the State only discovers information in relation to the reasonable grounds stipulated in search and seizure warrants. The Canadian Supreme Court did not accept this argument in its entirety and was of the opinion that search protocols are not always required in every case. The court was of the opinion that the judiciary is available for aggrieved suspects *ex post facto*. The court did, however, leave the door open that in certain cases *ex ante* search protocol requirements may be imposed and can become a requirement as case law develops. The court expressed the opinion that in certain cases, it can be necessary and practical to require search protocols specifically when confidential intellectual property or potential privileged information is involved. The court advised authorised officers that they should consider requiring *ex ante* search protocols or they should make use of a two-stage process whereby the police apply for a second authorisation after the original seizure in which searches are limited according to the strategies highlighted in search protocols. In this case, the court made it clear that the actions of the State will be examined *ex post facto* as to which and how many files were accessed and for how long. During an informal discussion with a member of the SAPS (2016) involved in crime investigations against the State, it was established that some members of this specific unit follows the process of conducting an original search for devices followed by obtaining a second search and seizure warrant setting out what information will be searched for on these devices.

If the practicality of only relying on *ex post facto* remedies is considered, one should take into account that with traditional search and seizures suspects have the right, but are not required to be present while their premises are searched. Although, as the court stated in the Polonyfis v.

Minister of Police and Others (2011) case, suspects do not have the right to prevent seizures from taking place if they think the terms of search and seizure warrants are exceeded. Suspects have the right to immediate legal recourse in applying to have a search and seizure declared invalid, based on what they witnessed during a search. If a search and seizure warrant permits the seizure of documents of company “ABC”, for example, and the suspects observed that the forensic investigators seized documents of company “XYZ” for no apparent reason, they have the right and the ability to immediately appeal the seizure. The argument is made that if forensic investigators do go outside the ambit of search and seizure warrants while analysing data in the absence of suspects and evidence is presented in a court case that falls outside the original search and seizure warrant, the legality thereof can then be tested during the trial (Kerr, 2005a:566). This argument is problematic − it places suspects in a position where they only know months or even years later when the trial starts that the forensic investigators went outside the ambit of the original search and seizure warrant.

Search protocols are the only mechanism that the court or suspects can evaluate to determine if forensic investigators will stay within the ambit of search and seizure warrants with their analysis of the data. A requirement can, therefore, be to require forensic investigators to specify what keywords they should use to locate relevant information (Guzzi, 2012:319) or to utilise independent filter teams to extract relevant information and only this information should be handed over to investigation teams (US Justice Department, 2009:110-111). This can place authorised officers in a position to determine *ex ante* if the ambit is going to be exceeded in relation to the information provided under oath upon which reasonable grounds exist to conduct the search. If forensic investigators have reasonable ground to believe that persons falsified invoices for company “ABC”, for example, it would be fair to specify keywords such as “ABC” and “invoice”, but if forensic investigators specify that they are also going to look for documents concerning company “XYZ” without indicating reasonable grounds regarding “XYZ”, then authorised officers can prevent this violation of constitutional rights *ex ante*. If forensic investigators, however, discover invoices of company “XYZ”, because the keyword “invoice” which was searched, this can be viewed as a legitimate discovery in plain view. A request was made by the suspect in the case of Gaertner and Others v. the Minister of Finance and Others (2013), that after the search and seizure of his computers, the search parameters should be properly defined, but his request was denied by the forensic investigators. Unfortunately, in this case all of the evidence was returned and a ruling was not made regarding the validity of this request. If the computer containing all of the data was seized and searched off-site without the suspect or his legal representative present, the whole argument of relying on *ex post facto* protection of the rights of suspects with regard to a search of the data falls short if no reviewable audit trail exists (Angermeier, 2010:1598). Audit trails should be so detailed that literally all actions taken by investigators while sifting through data, as specified in the Guidelines on

Disclosure for Investigators, Prosecutors and Defence Practitioners of the British Attorney General (2013:24-25), be recorded to place suspects in a position to protect their rights and place courts in a position to adjudicate on matters.

6.3.3 Intelligibility

One of the basic requirements for search and seizure warrants is that warrants should intelligibly define to both the searchers and suspects the ambit of these search and seizure warrants. Requirements to take into consideration concerning the intelligibility of search and seizure warrants were defined in the Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008) case, as:

- The authority under which warrants is issued, should be clearly stated.
- Searchers should be identified.
- The authority bestowed upon searchers should be clearly defined.
- Persons, containers or premises to be searched should be clearly identified.
- Suspected offences, which triggered a criminal investigation, should be clearly listed.

Although these aspects where identified as requirement of intelligibility in terms of the provisions of Section 29 of the National Prosecuting Act, Act (32 of 1998), the Constitutional Court in Minister for Safety and Security v Van Der Merwe and Others (2011) held that it saw no material difference between the National Prosecuting Act, (32 of 1998), and the Criminal Procedure Act (51 of 1977) and that, in this regard, it would apply equally to both.

From the recent High Court case, in the ruling of Heaney v. S (2016), which supports the ruling of the Supreme Court of Appeal in both the case of Polonyfis v. the Minister of Police and Others (2011) and Goqwana v. the Minister of Safety NO & Others (2015), it was made clear that search and seizure warrants should identify police officials who execute search and seizure warrants. In the Goqwana v. Minister of Safety NO & Others (2015) case, the appellant argued that due to the fact that the police official was not specifically identified, the search and seizure warrant was overbroad. The court considered that both Section 21 and Section 25 of the Criminal Procedure Act (51 of 1977) refer to “a” police officer and “such” police officer – pointing to a specific individual. The court held that this approach was also correctly interpreted in the case of Naidoo and Another v. the Minister of Law and Order and Another (1990) and in the

Smit and Maritz Attorneys v. Lourens NO and Others (2002) case. The court ruled in favour of the appellant and based their decision on the fact that police officials should be named to safeguard against abuse − suspects can then accurately identify police officials and reinforce the principle of accountability.

A further conclusion was made in the Goqwana v. the Minister of Safety NO & Others (2015) case − supported in the Heaney v. S (2016) case − that the suspected crime should be accurately described. In this case, the crime was described as "possession of illegal precious metals". The court ruled that it is beneficial when descriptions of suspected crimes in search and seizure warrants are clearly defined − suspected offences should, therefore, be accurately described. In digital evidence, this ruling is important. Terminology, such as "hacking", should not be colloquially-used terms, when the correct description should be "illegal access to data" in terms of the Electronic Communication and Transaction Act (25 of 2002) and can lead to warrants being found unintelligible.

Following the Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008) case, it was ruled as a requirement that articles should be sufficiently described in order for searchers and suspects to understand, or it is expected that they should understand within reason what a search entails and which articles are susceptible to seizure. This requirement is met when articles are sufficiently described or enough information about possible articles to be seized is provided. However, in the case of Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008), the court held that search and seizure warrants cannot be drafted according to the level of understanding of each suspect and the test whether search and seizure warrants are intelligible is not subjective. The lawfulness of search and seizure warrants would then depend on the capacity of suspect to understand the content. Intelligibility should rather be based on a reasonable understanding. The court expressed the opinion that it is unrealistic to expect the terms of search and seizure warrants to place suspects in a position to determine exactly what can and cannot be seized or to define the scope in an absolutely exhaustive or perfect way. It is acknowledged that the more complex the crime, the more likely it would be that there is a difference of opinion between suspects and the State as to what should be covered by search and seizure warrants. Computers virtually always contain relevant and non-relevant information and, therefore, it is even more likely that differences of opinion can occur regarding the seizure of computers. In the case of Polonyfis v. the Minister of Police and Others (2011), the court held that it is ultimately the discretion of searchers to decide if articles fall within the scope of a search and seizure warrant or not, but decisions made by searchers are subject to appeal and scrutiny in court.

In South Africa, search and seizure warrants are not required to specify which items, containers or filing cabinets will be searched on a premises. Section 21 of the Criminal Procedure Act (51 of 1977) only states that warrants authorise police officials to enter a premises and to search for identified articles. Warrants do not require the forensic investigators to specify how each room will be entered and how each cupboard will be searched. In a literal way, it can be argued that the same applies to computers. If computers are specified as articles to be seized, the forensic investigators can search each and every folder and file as they see fit. In the Minister of Safety and Security v. Van Der Merwe and Others (2011) case, the court set out that only the persons to be searched or containers or the premises to be searched should be specified along with the items or articles to be searched for and seized. It is, therefore, acknowledged that if search and seizure warrants define that houses may be searched to locate and seize invoices regarding "ABC" and no reference is made to computers − aside from privacy and overbroad issues − forensic investigators should be permitted to search computers found on the premises as possible containers of invoices regarding "ABC" in terms of Section 20 of the Criminal Procedure Act (51 of 1977).

The advantage of conventional search and seizure warrants is that the issuing authorised officers can evaluate the level of intrusion and can limit intrusion to specific areas of importance to the search. Suspects can also easily evaluate – when present − that law enforcement is staying inside the ambit of a search and seizure warrant. However, with search and seizure warrants for digital evidence many of these aspects are omitted and the technical level of understanding of authorised officers, suspects and investigators cannot be ignored. The question is then asked, if the authority to seize computers is not mentioned at all in a warrant, as per the given scenario above, will the reasonable person understand that the State is permitted to remove computers containing all of the data, create forensic duplicates and search through the data off-site? Secondly, will a reasonable person understand that the scope of forensic duplicates entail that all files − even deleted files – are duplicated and not only relevant files? Computers have become such an integral part of our lives and in the commissioning of crime (SALRC, 2010:7), that it seems logical for forensic investigators to clearly state and request the seizure of the computers containing all data, if it is reasonably believed that these computers contain evidence relevant to an investigation. However, it should also be known beforehand if digital forensic investigators are going to be available on a the scene to create forensic duplicates or if the computers will have to be removed from the scene as prescribed by the SAPS Interim Standing Operating Procedures Dealing with Electronic Evidence (SAPS, 2016:12)

It is acknowledged that the State does have access to warrantless seizure authorisations in terms of the provisions made in Section 22 of the Criminal Procedure Act (51 of 1977), but this

research study is limited to search and seizures with warrants. In light of the fact that computers have become a reality in almost all criminal investigations, it would be a detrimental oversight to rely continually on Section 22 of the Criminal Procedure Act (51 of 1977) when computers are encountered on a scene when a search and seizure warrant is being executed. This statement is in line with the ruling of the Constitutional Court in Gaertner and Others v. the Minister of Finance and Others (2013) case, where the court ruled that exceptions to the requirements of warrants should not become the rule and the court warned that search and seizure warrants are not a mere formality. It was further supported by comments made by the Supreme Court of Appeal in the case of Goqwana v. the Minister of Safety NO & Others (2015), that search and seizure warrants should not be considered as a mere "checklist approach". In the recent case of Gumede v. S (2016), the Supreme Court of Appeal found that if there is sufficient time available, search and seizure warrants should be obtained.

In the United States v. Hill (2006) case, the applicant argued that it was a failure on the side of the State to explain the technical reasons why an onsite search was impractical since the technical knowledge of the authorised officer who approved the search and seizure warrant was unknown and it was, therefore, unsure if the authorised officer applied his mind correctly and made an informed decision. The Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations of the United State Department of Justice (2009:78) advise that since the imaging and removal of computers are necessary in virtually every search where digital evidence is sought, it is doubtful that the omission of this fact in applications of warrants would violate the constitutional rights of persons, but it is nevertheless a good practice to include technical knowledge in applications since it demonstrates that the requirements of the Fourth Amendment are satisfied.

In the Constitutional Court case of the Minister of Police and Others v. Kunjana (2016), the court held that the more a search intrudes on the "inner sanctum" of persons, such as the homes of persons, the more the search infringes on the rights of persons and the forensic investigators can intrude in instances where the expectations of privacy are very high. The apex of the expectations of individuals with regard to privacy on their computers and mobile devices was recognised in the Canadian case of R. v. Vu (2013), where the court set aside a search and seizure warrant since it did not explicitly mention that computers would be searched and seized. The complexity of computers prompted the court to overrule the previous ruling that found that computers are no different than filing cabinets on a scene and that investigating officers are authorised to conduct a reasonable examination of everything at a location where articles can be found. The complexity of computers often leads to individuals comparing computers to familiar physical world objects and the unique nature of computers is completely ignored – individuals are trying to fit a square pin in a round hole (McLain, 2007:1072). The Supreme

Court of Canada held in the R. v. Vu (2013) case that computers are very different than filing cabinets. When computers are considered in the same light as filing cabinets, not enough attention or consideration is given to the unique privacy concerns that computers pose. After exploring the unique aspects of computers, the court held that the search for digital evidence warrants a distinctive treatment under Section 8 of the Canadian Charter of Rights and Freedoms and that specific prior authorisation must be obtained for searches where computers are involved and as such, search and seizure warrants must specifically specify the authority to search computers.

The aspect of intelligibility equally applies to both searchers and suspects. For the purpose of this study, a practical distinction is made between the use of the term “search”, meaning “locating”, “analysis”, or “interpreting”. This distinction is required to point out that data can be searched automatically to locate relevant information without the content becoming known and secondly, once relevant information is located, it can be read, analysed or interpreted as part of an investigation. This is the basis of an “exposure-based approach”, which proposes that data is only considered searched when data is exposed to human observation (Kerr, 2005a:547). If search and seizure warrants, therefore, allow forensic investigators to locate computers on a scene and the seizure of and an off-site search of data is permitted, it can be argued that a search has not yet been concluded when devices are removed from a scene. The search for specified devices is completed, but the search for relevant data on these devices has not yet been performed (Kerr, 2005b:100-108). This raises two aspects, namely at what point does search and seizure warrants expire – are additional searches for relevant data on devices part of “on-going” search and seizure warrants? Secondly, if a search for computers is performed by a forensic investigator on a scene while a search through the data is performed by a digital forensic investigator away from the scene, who is the “searcher” referred to in terms of intelligibility? A strong argument can be made that the forensic investigator and the digital forensic investigator can both be perceived as the “searcher” since the forensic investigator is normally not present in digital forensic laboratories when data is searched. Although it was found in the Goqwana v. the Minister of Safety NO and Others (2015) case that the searcher should be identified in search and seizure warrants, it was also held that in many situations, the searcher will have to be assisted by other investigators, but at least one of the police officials responsible for a search should be identified. This will, therefore, permit digital forensic investigators to also act as secondary or removed searchers without being directly identified in a search and seizure warrant. It is, however, advised in the Practical Guide of the SAPS (SAPS, 2016:10) that the name of digital forensic investigators should be included in search and seizure warrants, but only for purposes of their presence on the scene. If a digital forensic investigator is recognised as the searcher, it can be further argued that the search and seizure warrant is the only document from which the digital forensic investigator should determine what is included or

excluded for his “search” through the data and no other “external sources” should be used. This approach is inline with the ruling in the Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008) case that “it may therefore be said that the warrant should itself define the scope of the investigation”.

6.3.4 Overbroad seizures

The validity of search and seizures is assessed by both reviewing the content of search and seizure warrants and the actions of the State during the execution of search and seizure warrant – as landmark case, Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008) can be provided as South African example with regard to the legal aspects of search and seizure warrants. In terms of overbroad search and seizure warrants, the court held that search and seizure warrants should be specific enough that both searchers and suspects know or should have known what is being searched for and articles should be sufficiently described within the bounds of the empowering statutes. Search and seizure warrants should specify their goal and no reliance on external sources should be required.

Because of the fact that suspects can easily hide evidence, it has been recognised that forensic investigators are required to seize and search entire computers to “effectively execute” search and seizure warrants (Lowenstein, 2007:1). Unfortunately, this requirement seemingly carries a search outside the normally accepted ambit of traditional search and seizure warrants that focus on balancing the interest of the State with the interest of suspects. This is specifically true while concerns regarding constitutional rights are amplified, when the State is conducting comprehensive searches, which often unearth private, privileged and non-relevant information as well (Lowenstein, 2007:1).

In the case of Polonyfis v. the Minister of Police and Others (2011), the court explained that search and seizure warrants should be sufficiently clear concerning authorisation. When warrants are too vague, it is not possible to determine whether they extend outside of the statute of authority or not. The court referred to overbroad warrants in this context. In light of the above, it is, therefore, necessary that articles listed on warrants should be clearly described. The question is whether only physical devices should be described or data as well or both and to what detail?

The United States Department of Justice (2009:71) specifies that investigators should apply their mind in terms of what the subject of their search and seizure should be − data or physical computers. In some cases, computers are the items to be seized since it may not be legally

possessed due to, for example, child pornography stored on the computers. In this situation, computers cannot be forensically duplicated and left on a scene since the possession of child pornography is an offence that continues and computers may not be left lawfully in the custody of owners. It should, therefore, be specified in applications of search and seizure warrants if data is viewed as the subject of the seizure or the physical computers. If data is specified as the subject in a search and seizure warrant, the data should be sufficiently described in relation to suspected offences − not too overbroad or too sweeping − but also not too narrow that the State is prevented from conducting sufficient investigations. Overbroad classifications of data should be prevented, such as “all records” (United States v. Ford, 1999) or “any and all records, but not limited to” (United States v. Fleet Management Ltd. 2007). In the case of Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008), the court held that a “catch-all” phrase was permissible in this case since it was unreasonable to expect of investigators to describe all possible classes of documents when crimes are broad and complex. This was also permitted by the court in the case of the Minister of Safety and Security v. Bennett (2007), specifically when an extensive collection of physical documents are seized. The court held in the case of Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008) that using a “catch-all” phrase within search and seizure warrants to “authorise a wide-ranging search through all an attorney’s documents, files and computers” was overbroad. The United States Department of Justice (2009:74) further advises that the description of data should not be limiting in terms of the types of files, such as MS Word documents or spread sheets, but should rather be described as “records” and “information”.

Kerr (2005b:102) expresses the opinion that if you only describe computer hardware to be found on a crime scene, you are technically correct, but in seizing computers containing all of the data is too overbroad since the computers contain a magnitude of non-relevant information. In addition, digital forensic investigators are then left in the dark as to what exactly to search for once these computers are accessed. This aspect can also have an impact on the intelligibility of warrants, as discussed previously. If only relevant data is described, a search and seizure warrant is more focused and cured of an overbroad description, but in light of all the practical problems involved, such as the possible encryption of evidence and the sheer size of data, it is virtually impossible to complete a search on a scene. In this case, the search and seizure warrants will not encompass all of the actions planned by forensic investigators when computers containing all of the data is seized and removed.

On examining the Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) case, it seems that search and seizure warrants are defective on a number of issues. In the above-

mentioned case, the search and seizure warrant did not specify the offence, but merely stated "documentation, which is on reasonably grounds believed to be intended to be used in the commission of an offence". Secondly, the search and seizure warrant made provision for the seizure of "any computer hardware containing information relating to the above-mentioned entities" relating to a number of trusts and companies. Again no identification was made of the types of documents, how they were believed to relate to the crime, or evidence that was supposedly believed to be stored on the computers and also no period or cut-off date was specified. These complications caused the court to conclude that the search and seizure warrant was too vague and overbroad. In executing this specific search and seizure warrant, the SAPS seized virtually the whole computer collection and retained these computers for several days to conduct an "off-site" search. It was later acknowledged that the majority of articles seized, contained no relevant material. The State argued that there was "nothing untoward or strange" about this approach and that it has become the international standard way to conduct search and seizures for digital evidence. It was reasoned that the search was conducted off-site to minimise disruptions caused to the business of the suspect. The court held that this approach was not authorised by the search and seizure warrant, since the search and seizure warrant only authorised the search and seizure of "documentation" while Annexure A of the search and seizure warrant specified computers and peripherals, which the court held could "by no stretch of the imagination" be classified as "documentation". The court also held that no mention was made in the search and seizure warrant of conducting an off-site search and that the Criminal Procedure Act (51 of 1977) does not sanction the seizure of articles not described as Section 20 articles of the Criminal Procedure Act (51 of 1977) or on reasonable grounds believed to be articles concerned with the commissioning of a crime or viewed as evidence of the commissioning of a crime or intended to be used in the commissioning of a crime. The Court further held that it was unnecessary to remove the computers since they could have been "effectively searched and copied at the premises" within a few hours and it should be of the utmost importance that searches of this type be carried out in the least restrictive manner.

In studying the ruling of Beheersmaatscappij and Another v. The Magistrate Cape Town (2004), it was determined that the primary reasons for setting the search and seizure warrant aside was that the suspected offence should have been identified and a clear indication of the types of evidence, documents or articles relating to the offence should have been provided and not just documents or files related to the parties involved. An indication of the period under investigation or a "cut-off date" should also have been provided. These primary reasons provided by the court for setting the search and seizure warrant aside, was also highlighted in the Imperial Crown Trading 289 (Pty) Ltd v. Birch NO and Others (2012) case where the court held that the data which were sought was not limited by any time period and the SAPS gained, therefore, unlimited access to all of the data. It is, therefore, evident that courts require reference to the

categories or classes of articles in the body of search and seizure warrants and these references should correspond with the descriptions of articles in subsequent annexures.

Actions taken by investigators should be specified and authorised by search and seizure warrants. The court held in the case of Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) that the off-site search was not mentioned in the search and seizure warrant. From the verdict it cannot be determined if the court would have sanctioned an off-site search if it was stated in the search and seizure warrant. The court mentioned in the case of Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) that the state was unable to refer to a South African authority in relation to an off-site search, and indicated that the quoted international authorities were not helpful. From the research South African-based authority was located in the case of Minister of Safety and Security v. Bennett (2007), which is similar to the American case of United States v. Tamura (1982), where the blanket seizure and off-site search of 400 000 physical documents were held to be lawful.

An important aspect was touched on in the Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) case, namely that consent given by suspects to allow the State to create a full system “mirror copy” under the belief that the SAPS are allowed to act as they are, cannot validate irregular search and seizure warrants. A further aspect pertains to the fact that consent should be given voluntarily − without being influenced or under implicit threat or show of force (Basdeo, 2009:104). This aspect was further supported in the case of Powell NO and Others v. Van der Merwe and Others (2004) where the court held that the consent given by the suspect was not given voluntarily, but under duress − the SAPS stated that if consent is not given to permit an entry and a search of the premises, a search and seizure warrant will be obtained. It is reasoned that similarly the statement of the police in the Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) case, that if the suspect do not consent to the creation of forensic duplicates, the police would seize and remove all the computers, would also constitute consent under duress.

An additional aspect that should be considered is who decides what the least restrictive route is to follow: the seizure and removal of the computers containing all of the data or the forensic investigators staying on the scene for a prolonged period of time. The assumption can be made that the least restrictive route should be followed concerning the aggrieved party, in other words, suspects, but in practice it is found that the forensic investigators decide. This assumption is in line with the court ruling in the case of Polonyfis v. the Minister of Police and Others (2011) where the court held that suspects cannot prevent a search from taking place or in what format a search takes place, but it is ultimately the discretion of searchers to decide − knowing that their actions and decision are subject to appeal and later scrutiny in court.

In dissecting the Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) case, it is concluded that this case does not provide clear guidance with regard to if the information which is subject to the investigation was described as well as the physical devices and if this is in line with the authority provided in the statute and if the forensic duplicate or seizure of the computer containing all data is permissible or overbroad. The reason why the seizure of computers containing all of the data is judicious, was discussed in chapter two. In the case of Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008), the reasons for and the practice of creating forensic duplicates and the seizing of identified computer devices found on the scene containing relevant files, were not questioned. What was, however, scrutinised was the "catch-all" paragraph in the search and seizure warrant, which in essence, stipulated that investigators were also allowed to − subsequent to the listed items and articles − also search and seize any items or articles that can have a bearing on the investigation. The court held that this "catch-all" paragraph was permitted in this specific case, but in terms of the search concerning a legal practice, the "catch-all" paragraph allowed a wide-ranging search through all of the documents and this opened the door too widely and provided insufficient direction to searchers and the suspects and the paragraph was, therefore, overbroad. The court only referred to the search through all of the documents and not the seizure of all of the documents, which is similar to the ruling in the case of the Minister of Safety and Security v. Bennett (2007) in which the seizure of a large collection of intermingled documents for an off-site search was permitted. The SAPS implemented mechanisms to manage subsequent searches of documents and the court ruled that these mechanisms did not cause any prejudice concerning suspects.

If search and seizure warrants are found to be overbroad or defective, South African courts will strike these warrants down completely or only the defective portions, if defective portions of the search and seizure warrants can be severed from the rest of the warrant. The Court compared the declaration of the whole search and seizure warrant as invalid, if only a portion of it is defective, to using a sledgehammer to crack a nut (Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others, 2008). The practical aspect of this is that if computers containing all of the data is seized and it is found that the seizure of all of the data on these computers was overbroad, how will the data seized outside of the scope of the search and seizure warrant be severed from the rest?

When forensic duplicates are created of computers containing all of the data, no files can be added or removed from the forensic duplicates. This aspect adds to the trustworthiness of the process (Casey, 2011:60). Even if files are deleted on a scene or thereafter, it is still possible for digital forensic investigators to recover these files (Cross, 2008:140). This situation places

forensic investigators in an unattainable position, especially in cases where computers are involved. If only relevant data may be forensically duplicated and not all of the data on a computer based on, for example, a keyword search, none of the system-related information will be forensically duplicated, but only files containing keywords. This can be severely detrimental to the interest of justice in a number of ways. Firstly, evidence can be interpreted incorrectly. Secondly, the forensic investigators may be unable to place the evidence in context, especially if the defence has the advantage of having access to all of the data on computers and pose questions or make allegations outside of the ambit of what the forensic investigators were allowed to seize. The British Attorney General's Guidelines on Disclosure: Supplementary Guidelines on Digitally Stores Material (2011:10.) also points out that if all data is not copied, investigators will not be able to locate and analyse evidence pointing away from the guilt of suspects. This is an extremely important aspect. An example of where such a principle can count in the favour of suspects, is where the SAPS are searching for child pornography and they are only permitted to seize the child pornography. Once found, suspects can be found guilty for possessing child pornography, but if the SAPS seized all of the data on the computers, they would have discovered that these computers were infected with a malicious program which was downloading child pornography without the knowledge of users.

6.3.5 A two-step process and off-site searches

International courts have grappled for years with the unique complexities that digital evidence pose to search and seizure and have attempted to apply constitutional constraints on search and seizure warrants (Bartholomew, 2014:1027). The goal is to strike a fair balance between the interest of the State in maintaining law and order and the constitutional rights of suspects (Bartholomew, 2014:1028). Unfortunately, there is no clear guidelines or rules for forensic investigators to follow. Chan (2014:442) uses the analogy of the needle and the haystack to describe the practical side of the search and seizure of digital evidence. Chan differentiates between two distinct phases, namely the data acquisition phase and the data reduction phase and compared the acquisition phase with collecting the haystack and searching for the needle as the reduction phase.

In the Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) case, the State stated that seizing the computers and conducting an off-site search have become the standard way of searching and seizing computers in South Africa and elsewhere in the world, but the court ruled that seizing computers and conducting an off-site search were not permitted, according to the Criminal Procedure Act (51 of 1977). If computers are not an article in terms of Section 20 of the Criminal Procedure Act (51 of 1977), the court stated that computers cannot be seized and removed from a scene. The implication is that computers should be searched as

filing cabinets on a scene. This procedure will, however, have a negative impact on the integrity of evidence if a search is completed incorrectly. If investigators, for example, open files and print them, the action is viewed as not neutral and influences the evidence (Vacca, 2005:19). The Explanatory Report to the Cybercrime Convention points to the fact that digital evidence should be retained in the state it was found from when a search commenced to when prosecution takes place (Council of Europe, 2001b:38). Kessler (2010:6) points out that each stage of this process should be performed in such a way that the integrity of evidence is preserved.

The Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) verdict has a potentially far-reaching impact on digital forensic search and seizure in South Africa. No specific remedy for the perceived conundrum that digital forensic investigators face was proposed (McLain, 2007:1083). On the one hand, industry guidelines, such as the ACPO's Good Practice Guide for Computer-Based Electronic Evidence (1997), dictate that the actions of investigators should not change or alter evidence, yet a traditional approach dictates that the evidence should be searched on the scene prior to being seized.

Search and seizure rules in the United States of America was based, as in South Africa, on a one-step process whereby law enforcement enters an identifies premises and seize listed articles, for example computers listed in the search and seizure warrant. Kerr (2005:86) argues that new criminal procedures are necessary to effectively govern the complications digital evidence pose. Existing search and seizure rules should adapt. The traditional one-step process should be replaced with a two-step process, which includes forensic investigators entering premises, seizing the listed hardware, taking the hardware off-site to search for relevant data (Kerr, 2005:87). Kerr expresses the opinion that the failure of law enforcement to account for a two-step process with the search and seizure of digital evidence is causing a great deal of doctrinal confusion making it difficult for the law to regulate the process of digital warrants effectively.

A distinct differentiation can, therefore, be made between these two search processes. The one occurs at the original premises of suspects and the second normally at digital forensic laboratories of law enforcement. These two processes take place at different times and can be executed by different people. It should be noted that normally the search step of data is performed after a seizure took place and at the location of forensic investigators (Kerr, 2005b:85). During a normal process, articles can only be seized after a search action was performed in terms of searching for and seizing physical computers, but data is seized before the information is searched (Chan, 2014:442). The logical consecutive sequence of search and seize is, therefore, abandoned when the focal point is data. It is recognised that data can be seized prior to being searched (Brenner & Fredericksen, 2002:82).

The motivation for permitting off-site searches is based on the fact that the seizure of large volumes of documents − as generally found on computers − deprives owners of the ability to access these documents and can require forensic investigators to stay on a scene for prolonged periods of time − weeks or even months. This is viewed as intrusive with regard to suspects and burdensome for forensic investigators (Welty, 2011: 9). Upon showing the necessity to an authorised officer, a forensic investigator should be permitted to create a forensic duplicate of the whole collection of data and to conduct an off-site search (Angermeier, 2010:1615). This statement is supported by Bartholomew (2014:1035) who provides additional motivation for the practice of conducting a broad seizure of computers followed by an extensive off-site search. Reasons can be summarised as follows:

- It can be very time-consuming to conduct thorough searches of computers and these searches can take days, weeks or even months due to the storage sizes of computers.

- Suspects can easily hide, encrypt, password protect or destroy evidence to hinder investigations.

- Relevant data is not always located in files, but can be stored within system files or computer generated records.

In the American case of Davis v. Gracey (1997), the court found that to search computers on-site is more disruptive than searching computers off-site. The court found it “obvious” that searching computers for evidence requires great skill, time and expertise. It was, therefore, found that it is more reasonable to conduct off-site searches than staying at the house of a suspect for a number of days conducting a search. In the United States v. Hay (2000) case, the seizure of physical computers was found lawful due to the “time, expertise and controlled environment required for a proper analysis”.

The need for allowing a two-step and off-site search process is widely recognised in the industry, by academics (Kerr, 2005b; Welty, 2011; Bouwer, 2014), court cases and regulatory guidelines (US Department of Justice, Guidelines for Searching and Seizing Computers and Obtaining Electronic Evidence for Use in Criminal Investigations and the British Attorney General’s Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners).

In 2009, Rule 41 of the Federal Rules of Criminal Procedure (2009) was amended by inserting Rule 41(e)(2)(B). This amendment is in line with Kerr’s proposal and this rule states that search and seizure warrants may authorise a seizure or a forensic duplication of digital evidence and a later review of data. The Committee Notes on Rules (Cornell University Law School, n.d.) explains that due to the fact that computers contain large quantities of intermingled information,

it is impractical to conduct a search on a scene and an overbroad seizure is, therefore, permitted followed by an off-site search. This process was justified by practical concerns.

The lawfulness of an off-site duplication of a computer was recognised in the unreported judgement of the then Transvaal Provincial Division of the High Court, case 10828/2005, where the court held that “it does not matter where a back-up of a hard drive is made”.

The use of language in the applications of search and seizure warrants in permitting or justifying overbroad seizing of articles stems from the case of the United States v. Tamura (1982). In this case, the State seized a large collection of boxes of physical documents, which contained innocuous documents due to the infeasibility of searching through all of the boxes on the site. The court expressed the opinion that in these types of cases of commingled documents, the State should avoid violating Fourth Amendment rights by obtaining prior permission to seize all of the documents to search off-site. A comprehensive seizure can, therefore, be “monitored by the judgment of a neutral, detached magistrate”. This is widely referred to as the “Tamura rule”. In 1994, Winick (1994:126-128) proposed that the Tamura rule should be applied to the seizing of computers due to the intermingled nature of information on computers and the controversy that surrounds privacy with regard to computers. Winick, however, expanded on the Tamura rule and proposed the following additional requirements:

- Courts should articulate specific search protocols setting out exactly how forensic investigators may search data.
- Forensic investigators should supply an outline of the methods to be used to sift through information.

Kerr (2005a:572-573) is of the opinion that the Tamura rule only required the State to specify where a search will occur and what will be seized while Winick extended the specifications to also include how a search will be performed.

In the United States of America, it has become practice under many investigators to use affidavits to obtain search and seizure warrants to explain to authorised officers the practical need why computers should be seized and removed from a premises to allow for an off-site search. By signing search and seizure warrants, authorised officers are in fact approving off-site searches (Kerr 2005b:110). Authorisation will, however, not prevent suspects from challenging the validity of search and seizure warrants.

In the case of the United States v. Hill (2006), the applicant appealed the seizure of his computers without the police conducting a search of these articles on the scene to determine if they contained data as described in the search and seizure warrant. The applicant argued that

the court erred by simply assuming that the difficulties of an on-site search were “well-known”. The Ninth Circuit Court agreed with the trial court that it is unreasonable to bring computer equipment to a scene to determine if the storage media contains evidence, but the court agreed with the applicant that the State had the burden to make at least a minimum showing why the blanket “seizure of the haystack is needed to search for the needle” and why an onsite search is impractical. It was argued that it was a failure on the side of the State to explain the technical reasons why an onsite search was impractical, since the technical knowledge of the authorised officer who issued the search and seizure warrant was unknown and it could, therefore, not be determined if the authorised officer applied his mind correctly and made an informed decision. McLain (2007:1081) is of the opinion that the court was incorrect in its conclusion − it is unreasonable to expect of the police to conduct an onsite pre-search or preview. If it is expected of the police to always conduct pre-searches or previews of computers on a scene, it can place the police in a position between two untenable situations – to either conduct a physical pre-search and damage evidence or make forensic duplicates and review the duplicates to establish if it contains evidence (McLain, 2007:1083). These situations are however not “black-and-white” situations. It is possible to connect the computers of suspects to a write-protector device that can allow the police to conduct searches for specific keywords derived from a search and seizure warrant to ascertain if the content stored on computers is covered by the search and seizure warrant without influencing the evidential value of the data. This approach is supported by the Australian Crimes Act (12 of 1914), Section 3K and 3F, which allows for investigators to bring specialised tools to search and seize digital evidence on a scene and provides that digital devices may be seized, but only if these devices have been sufficiently examined to determine whether these devices contain evidence. However, this option also poses problems to the State, since the police cannot know beforehand how many articles will have to be seized. The process of pre-viewing data is time-consuming and can be inconvenient for suspects to have the police on their location for a long period of time. Even if the police make forensic duplicates on a scene, a casual review of forensic duplicates will not ensure an accurate identification of evidence.

In the New Zealand case of the Director of Serious Fraud Office v. A Firm of Solicitors (2006), it was held − as in the Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) case − that although the computers were relevant to the search, it cannot be said that the computers themselves were articles of relevance and the seizure thereof was ruled to be unauthorised. The New Zealand Court further held that if the computers were cloned, they may only be removed if:

- the evidence cannot be removed other than by making use of forensic investigative techniques.

- it is not practical to carry the extraction out on-site without the risk of destroying the evidence or due to an unsuccessful extraction.

- there is no practical alternative to removing the hard drives to conduct an off-site search.

The ruling of the court in the Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) case, simply stated that it was unnecessary and unauthorised to remove physical computers from the scene. From the research conducted, it seems that internationally it has been recognised that it is practically impossible to complete or conduct a full search of computers on a scene and strict guidelines and control measures are set in place to manage full searches of computers off-site. One of these controlling measures is the British Attorney General's Guidelines on Disclosure: Supplementary Guidelines on Digitally Stores Material (2011:5, 11) that provides for investigators to remove computers from a scene if it is not possible to duplicate data stored on computers on a scene and to conduct an off-site search. Investigators are, however, cautioned not to remove more material than what is justifiable.

The United Kingdom-based guidelines provided in PACE 2001 (Health and Safety Executive, 2014), state that investigators should consider only making printouts from computers, but if a case requires a greater interference in terms of the provisions of Section 20(2)(m) of PACE 2001 (Health and Safety Executive, 2014), the power should be carefully considered if additional actions are necessary, justified and proportionate. These guidelines propose that alternatives to seizing physical computers in cases where computers contain a large amount of relevant data, creating and seizing forensic duplicates should rather be considered, since the seizing of physical computers greatly limits owners.

Division 2 of the Australian Crimes Act (12 of 1914) Section 3K allows for the removal of articles to a different location if the creation of forensic duplicates on a scene is not practically possible, but these articles should be returned within 14 days. An extension can be requested for up to seven days at a time. Investigators should provide owners with an address to where articles are removed and owners or representatives can be present during an inspection of these articles.

In the case of Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008), the search and seizure warrant under scrutiny stipulated that forensic duplicates will be made of the evidence and thereafter "at a location removed from the premises" evidence will be retrieved by means of a forensic analysis. This aspect was not scrutinised by the court. In the unreported judgment of the then Transvaal Provincial Division of the High Court, case 10828/2005, the court provided a clear verdict on this aspect and held that "it does not matter where a back-up of a hard drive is

made". It was further explained in this case, that the Computer Crime Investigation Unit of the SAPS functions the same way as independent filter teams and only extracts and hands over relevant information to investigators. The court stated: "I am satisfied that no more information would have been conveyed to the respondent than was covered by the warrant". During an unstructured interview with a former police officer, it was established that this process is not followed anymore, but that all of the data is handed over to investigators (Anon, 2016a).

The protection of the constitutional rights of individuals depends upon investigators policing themselves if individuals are not present during a search and seizure (Chan, 2014:450). It is, therefore, required to consider the rights of suspects when off-site searches of articles are permitted. This issue does not relate to suspects being present when data is analysed or when additional investigations of a case take place, but refers to the phase when data is searched to locate relevant or non-relevant information.

A request was made in the Gaertner and Others v. the Minister of Finance and Others (2013), case to restrict investigators of the South Africa Revenue Services to only duplicate and seize data in the presence of the suspect. This request was declined, but the undertaking was given that data should be seized and only extracted in the presence of the suspect. Section 21 of the Criminal Procedure Act (51 of 1977) does not require suspects to be present during a search and seizure and authorises the SAPS to search a premises in the absence of suspects. Suspects may not be refused access to premises to be present when their property is searched when they do not commit additional crimes or obstruct the search. If data is not searched on a scene and no segregation of relevant and non-relevant data has taken place, then suspects should have the right to be present during a search of the data. Suspects can assert their right to monitor a search to make sure that the forensic investigators stay within the ambit of the search and seizure warrant. The review of data on a seized computer is recognised as a "search" in the case of the United States v. Syphers (2005) and that the search of data is a continuation of the search (Department of Justice, 2009:86-87). This approach is permitted in the United Kingdom, according to Section 53 of the Criminal Justice and Police Act (16 of 2001) that states that seized material should be examined as soon as practically possible to determine what should be retained and what not. The desirability of allowing owners to be present should be considered, but not precluded.

6.3.6 Duration of seizure to create forensic duplicates and retention of non-responsive data

Three retention periods are discussed in this section, namely:

- What time is reasonable when computers are seized from a scene until forensic duplicates are created and originals returned to suspects?

- If physical computers are seized or forensically duplicated, what period is reasonable to conduct a search of the data to identify related and non-related information?

- Is there a time requirement set on how long an analysis of data should take?

During an unstructured interview (Anon, 2016a), it was established that there are no parameters set in terms of retaining seized computers other that the Criminal Procedure Act (51 of 1977). The interviewee mentioned that the DPCI is able to − after cellular phones were seized – to return these phones generally within a week and computers generally within two weeks, but in cases with larger quantities, generally before two months. In the general SAPS, it takes generally closer to two months on average (Anon, 2016a).

In South Africa, the Criminal Procedure Act (51 of 1977) does not make any mention of a time limit in days with regard to the three identified retention periods. Instructions in terms of the disposal of articles are provided in Sections 31, 32, 34 and 35 of the Criminal Procedure Act (51 of 1977). The State is, therefore, allowed to seize computers and to keep these computers for an unspecified period of time. Suspects are, therefore, placed in an undesirable position – they have to rely on the State to act in utmost good faith or suspects can turn to the courts and apply for an urgent application to have their property returned. In the United Kingdom (British Attorney General, 2013:20-21), it is a requirement that computers should be forensically duplicated on a scene or seized. Investigators should consider the impact of this requirement on seizing large quantities of computers when forensic duplicates cannot be created on a scene and within what timeframe these computers should be returned. Forensic duplicates should be made as soon as reasonably possible. Although the seizure of forensic duplicates is permitted, no additional material may be removed than can be justified and non-relevant material may not be retained. In the United States of America, a limitation of fourteen days is placed on investigators by Rule 41(e)(2)(B) of the Federal Rules of Criminal Prosecution (2009) to “execute” search and seizure warrants. This relates to the seizure of computers or on-site forensic duplications made of data and no additional off-site duplications of data or searches for evidence. The United States Department of Justice further advises that forensic duplicates should be created and originals should be returned within a reasonable time (2009:247). The Australian Crimes Act (12 of 1914) Section 3L makes provision for investigators to secure computer equipment for an examination or to create forensic duplicates that take up to 24 hours, which should be sufficient with modern-day duplication processes to create forensic duplicates. Section 3K of the Australian Crimes Act (12 of 1914), allows for devices to be seized and removed, but these devices should be

returned before 14 days. Extensions of no more than seven days at a time can be requested. Although no defined period is found in the South African legal environment for a reasonable period after seizing computers to create forensic duplicates and returning originals to owners, the court held in the Beheersmaatscappij and Another v. The Magistrate Cape Town (2004) case that the SAPS had no power to seize a large collection of computers from the suspect and to retain these computers for a "few days". The business of the suspect was disrupted more than what was necessary. Although no indication of a reasonable period was given in days during this case, the return of original devices within a reasonable period of time should be viewed as a priority.

If the broad seizure of digital evidence is permitted, what period is reasonable for a search of the data to locate related and non-related information and to review or analyse data. In the case of the United States v. Hernandez (2002), the court held that neither the Federal Rules of Criminal Procedure (2009) nor the Fourth Amendment placed any specific limit on the duration of the State's analysis of digital evidence. In this case, the court expressed the opinion that similarly to a search and seizure warrant for voluminous documents, if the documents are seized within the allowed period, the retention thereof and the prolonged review thereof does not automatically qualify the evidence for suppression or require applications for extensions or additional warrants.

Certain courts in the United States of America are of the opinion that the reasonable standards of the Fourth Amendment require forensic investigators to search computers to locate relevant information before too much time has elapsed (Kerr, 2005b:122,137). This requirement does not relate to analyses and additional interpretations of relevant data, but only to the period from seizure to the identification and segregation of relevant and non-relevant information. Kerr further expresses the opinion that courts can hold that warrants − which originally authorised an "overbroad" seizure – can become less reasonable as time elapses and no search is performed or a search is prolonged. In cases where computers are only storage devices, forensic investigators should be required to create forensic duplicates of data in a reasonable time of 30 days and return the original hardware to suspects. This course of action is advised if courts acknowledge that forensically sound duplicates are original records or accepted as originals. If computers are, however, viewed as articles that may not be legally possessed by persons, such as the possession of child pornography, Section 35 of the Criminal Procedure Act (51 of 1977) stipulates that these articles cannot be handed back to owners.

In a number of cases in the United States of America, courts held that a long delay in analysing seized data does not constitute unconstitutional seizures. Examples of cases, include the United States v. Brewer (2009), the United States v. Syphers (2005) and the United States v. Gorrell (2004). However, this aspect was taken further in the case of United States v. Metter

(2012), where forensic investigators seized the computer devices of the suspect, created forensic duplicates of these devices and returned these devices within the time specified. However, the State failed to conduct a review of the data for a period of 15 months. The suspect contended that the State's significant delay violated his rights to privacy under the Fourth Amendment. The court held that with the complexities computers pose to investigations, some flexibility is allowed to forensic investigators, but the State cannot be permitted to ignore its responsibilities. If this happens, the requirements of the Fourth Amendment lose their power within the digital search and seizure environment.

Section 35(3) of the Constitution (1996) affords persons the right to a fair trial and this right includes a trial that begins and concludes without unreasonable delay − also specified in Section 342A of the Criminal Procedure Act (51 of 1977). However, in the United States v. Triumph Capital Grp (2002) case, the court expressed the opinion that where a delay for the review of seized digital evidence was reasonable under the circumstances, such a delay does not make a seizure unconstitutional. The court further expressed the opinion that digital searches generally involve larger sets of documents than a normal search and seizure and requires a higher level of care that can contribute to a prolonged period of investigation.

6.3.7 Segregation of data

Computers can contain a vast amount of and a variety of intermingled documents (McLain 2007:1071). While paper documents are normally stored, well-organised with labels to indicate content, filed according to subjects or content, computer data can be stored unorganised and intermingled and sometimes file names do not relate at all to the content (Kessler, 2010:27). Relevant, non-relevant and privileged documents can be intermingled on computers without the possibility of investigators "separating the sheep from the goats" on a scene. It is found internationally, that law enforcement is generally permitted to carry out overbroad seizures by seizing computers containing all of the data or creating forensic duplicates of all of the data on computers, but they are not permitted to scour through devices indiscriminately (R. v. Vu, 2013). As soon as investigators realise that seized devices do not contain any relevant evidence, these devices should be returned to owners as soon as reasonably possible (New Zealand Search & Surveillance Act, 2012; British Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners, 2013:21; Canadian Criminal Procedure and Practice Section 490). A reasonably timeframe is also applicable in South Africa in terms of the provisions of Section 31 of the Criminal Procedure Act (51 of 1977). It is further specified in the New Zealand Search and Surveillance Act (24 of 2012) Section 161(1) that all forensic duplicates made of devices, which were found to contain no evidence, should be deleted, erased or permanently destroyed. It is accepted by implication that the destruction or return of

forensic duplicates and work products is included in Section 31 of the Criminal Procedure Act (51 of 1977).

No dispute is perceived with devices that are found to contain no evidence, but the complication is highlighted with regard to devices that contain evidence and non-related information – which would be the majority of cases in terms of digital evidence. The British Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners (2013:22) make provision for when evidence or relevant material is inextricably linked to non-relevant material and it is not reasonably practical to separate relevant material from non-relevant material – then these devices can be retained. The test is whether the material can be removed without prejudicing the use of relevant material in a judicial process. It is strongly stated that inextricable-linked material may not be examined further, may not be further forensically duplicated or used for any purpose other than validating the integrity of relevant material. This approach is supported in the New Zealand Search and Surveillance Act (24 of 2012) Section 161(2). During an unstructured interview (Anon, 2016a), it was established that the current practice in South Africa does not distinguish between searching data to firstly only identify relevant information based on the ambit of search and seizure warrants, but in many cases all of the data created by users found on computers are handed over to investigating officers (Anon, 2016a). This is in contradiction to the court ruling in the unreported case of the then Transvaal Provincial Division of the High Court, case 10828/2005, where the Computer Crime Investigation Unit of the SAPS acted as an independent filter team and only supplied information to the investigator which was found to be within the ambit of the search and seizure warrant. Angermeier (2010:1598) is of the opinion that actions by forensic investigators searching computers cannot be easily reviewed by courts in relation to the violation of the rights of suspects. Although it is acknowledged by the British Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners (2013:25), it may be necessary to carry out sampling and searches on more than one occasion. This reference should be viewed in light of the prior condition that limited the retention of seized data to data that contain relevant information. It is argued that if evidence that falls outside a search and seizure warrant is presented as evidence against suspects, it would be easy to request the setting aside of evidence (Kerr, 2005a:583). This approach does not reflect the body and soul of the South African Constitution, in that the State expects persons to postpone their claim to their constitutional rights to the point where they discover months or even years later what evidence the State selected to use against them just because the digital medium in which the evidence was seized permitted the State to seize more information than what should actually be permitted. The constitutional rights of persons can only be breached by obtaining a warrant, which sufficiently describe only the articles which has a bearing on the investigation (Basdeo, 2009:6). If articles are seized beyond the scope of search and seizure warrants, the State

cannot validate the legitimacy of seizing these articles and suspects have the right to claim their constitutional rights (Basdeo, 2009:109-110).

An applicable case in this regard, is the Minister of Safety and Security v. Bennett (2007) where a blanket seizure and off-site search of 400 000 documents were held as lawful, since it was impossible and impractical to effectively search all of the files on the scene to separate relevant files from non-relevant files. Because it was impractical to conduct a search or rather perform a segregation of relevant and non-relevant documents on the scene, the seizure of all documents was permitted to enable the State to secure evidence. The parties involved reached an agreement concerning the monitoring of the segregation of relevant and non-relevant data. The agreement was not that the suspect would be permitted to be present while the financial statements were later reviewed and analysed, but the suspect would be present to make sure that the ambit of the search and seizure warrant was correctly used to segregate the documents. Non-responsive documents are normally returned or requested to be returned in line with Section 31 of the Criminal Procedure Act (51 of 1977). After this process is completed, the police cannot have a second viewing of a physical document which was originally found to fall outside the search and seizure warrant and which was returned to the suspect without obtaining a new search and seizure warrant. This procedure is also prescribed in the digital environment by the British Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners (2013:22), where it instructs investigators to segregate relevant and non-relevant information, but prevents them for conducting further investigations into the non-relevant data.

6.3.8 Privilege

It is well-accepted that computers contain a multitude of data (Lowenstein, 2007:10) and some of the data may be privileged. As discussed in the Thint (Pty) Ltd v. National Director of Public Prosecutions and Others, Zuma and Another v National Director of Public Prosecutions and Others (2008) rulings, both the Common Law and the Constitution (1996) protect privileged information. The South African law recognises two types of privileged information of importance to forensic investigators, namely matrimonial privileged information and legally privileged information.

6.3.8.1 Matrimonial privileged information

Section 198 of the Criminal Procedure Act (51 of 1977) states that a spouse shall not be obligated in criminal proceedings to disclose any communication which the other spouse made to him or her during a marriage.

Communication also relates to email communication, as defined in the Regulation of Interception of Communication and Provision of Communication-Related Information Act (70 of 2002), which defines communication as both direct and indirect and further defines indirect communication as the transfer of information in the form of data messages or emails.

This privilege can only be claimed by a spouse receiving communication (Schwikkard & Van der Merwe, 2002:142) while Section 199 of the Criminal Procedure Act (51 of 1977) stipulates that a spouse shall also not be compelled to answer questions during a criminal proceeding which a husband or wife, under examination, may lawfully refuse to answer. With so many types of communication available between spouses and the quantity of communication taking place via email and online platforms, this can have a huge impact on the ability of law enforcement to freely analyse email communication of persons if police officers should constantly guard against matrimonial privileged information.

6.3.8.2 Legally privileged information

Legal privilege is probably the type of privilege which is most focussed on in court cases. It is well documented that legal privileged information may not be seized under a search and seizure warrant as was confirmed in the case of Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008) and SASOL 3 (Edms) Bpk v. Min van Wet en Orde (1991). The right to legal privilege affords persons an opportunity to fully and unrestrictedly discuss their case with their legal advisor and to afford them the opportunity of a fair trial as stated by the Constitution (1996).

Section 201 of the Criminal Procedure Act (51 of 1977) states that legal practitioners may only provide evidence in matters where they act for persons in their professional capacity if consent is given by such persons.

Legal privilege must adhere to certain requirements before it can be claimed namely:

- The legal practitioners should have acted in a professional capacity, (Danzfuss v. Additional Magistrate, Bloemfontein, & Another, 1981).
- Legal advisors should have been consulted in confidence (Danzfuss v. Additional Magistrate, Bloemfontein & Another, 1981).
- Communication should have occurred with the aim of obtaining legal advice (S v. Kearney, 1964).

- Advice should not have been obtained with the aim of committing a crime (Scholsberg v. Attorney General of the Transvaal and the Additional Magistrate, Johannesburg: In re R v. Sandig & Others 1936).

Historically, the practice with seizing legally privileged information entailed the sealing of documents when persons claimed privilege and these documents were then handed to a neutral person, such as the Registrar of the High Court (Heiman, Maasdorp & Barker v. Secretary of Inland Revenue, 1968). In the case of Bogoshi v. Van Vuuren NO; Bogoshi v. the Director Office of Serious Economic Offences (1993), the court held that the person who claims the privilege should be given the opportunity to remove privileged documents after these documents were seized.

In the New Zealand case, Director of Serious Fraud Office v. A Firm of Solicitors (2006) the court made further provisions if off-site searches are permitted:

- Search and seizure warrant must be issued in terms, which protect the privilege of the suspects.

- Search and seizure warrant must contain conditions to ensure that the suspect's non-relevant articles are not accessed.

- Issuing judges must be assured that there is no other option than permitting the forensic duplication of the complete hard drive.

The Court further commented that "extensive conditions" were needed to protect privileged material and that it might "even be appropriate" for independent lawyers to be present during search processes.

In the Minister of Safety and Security v. Bennett (2007) case, the SAPS seized a large quantity of documents and kept it sealed. After the seizure, the suspect raised the aspect of legally privileged information. All documents were sealed and could not be accessed by the SAPS. It was argued that due to the fact that the SAPS seized privileged documents, the seizure of even only one document containing privileged information would "render the whole execution of the warrant invalid". The court held that this did not render the whole search and seizure invalid and that there was no prejudice towards the suspect due to the manner in which the SAPS handled the documents.

Section 54 of the United Kingdom Criminal Justice and Police Act (16 of 2001) and the Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners (2011:23), prescribe that legally privileged information may only be seized if there is not a

reasonable practical way of separating privileged information from other information on a scene and if privileged information is seized, it should be kept separate from other seized articles/data. Independent lawyers should review privileged information and the investigation team may not have access to this information. This information may only be retained if the information is inextricably linked to relevant information and it cannot be separated on a practical manner from the rest of the information. In this situation, independent filter teams must be used to analyse the documents and they may only provide relevant information that does not contain legally privileged data to the investigation team.

In Lavallee, Rackel & Heintz v. Canada (2002) case, the Supreme Court set a number of search protocols or rules when a search was conducted on law offices. Investigators should indicate to authorised officers that:

- No reasonable alternative existed.
- Unless search and seizure warrants stipulate that no examination may take place immediately, all of the documents should be sealed.
- Lawyers and/or clients should be contacted at the time of execution and if they cannot be present, a member of the Bar should be allowed to observe the search.
- Independent lawyers should examine the documents to determine whether they contain privileged information.

6.3.9 Searching of zones and plain view discoveries

The SAPS National Standing order 2/2002 makes reference to the search of areas or places where it is impossible to find articles defined in a search and seizure warrant. (SAPS, 2002:13). This relates to an aspect, as described by Chan (2014:442) that if a search and seizure warrant is executed to search for illegal rifles, the forensic investigators are not permitted to search in, for example, a jewellery box, which is too small to hold a rifle. In the case of the Ontario Court of Appeals in R. v. Jones, (2011) it was argued that computers are indivisible objects and subject to a lawful seizure a full examination of all files is permitted. The unanimous verdict of the court, was that the search of computers pursuant to a search and seizure warrant must be limited to the reasonable and probable grounds which was established as the basis for the application of the search and seizure warrant. As was seen from the verdict in Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008), the catch-all phrase of “or anything which might relate to …” can very easily lead to a finding that the search and seizure warrant was overbroad and

unconstitutional. If forensic investigators, for example, have information to reasonably suspect that a search should not be restricted to only illegal firearms, but also to documentation regarding illegal firearms, it should be stated in the application and subsequent search and seizure warrant. Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008) supported this ruling where the court commented that if Section 29 of the National Prosecuting Act (32 of 1998) were interpreted literally, it would mean that investigators can examine and seize "anything whatsoever" which may be said to "merely be possibly relevant". The court held that a literal interpretation suggests that everything that has not yet been inspected falls in this category. This implies that Section 29 of the National Prosecuting Act (32 of 1998) authorises complete examinations of every single article on a premises to determine if these articles have bearing on a case. The court found that this seemingly unbounded power is inimical to the constitutional right of privacy. Instead, the court advised that this Section should be governed by the fact that searches should be conducted with strict regard to decency, order and to the fundamental rights of individuals to privacy and freedom. The court expressed the opinion that forensic examiners should keep this duty in mind even if nobody is present to observe their actions. This approach was also supported by the Canadian Supreme Court in R. v. Vu (2013) where the court expressed the opinion that a search and seizure warrant does not give the police "a licence to scour a device indiscriminately". Instead, the court instructed that if the police, in the course of a search, realise that there is no reason to search a specific file or program, they should refrain from doing so.

When authorised officers approve applications for search and seizure warrants, it is done on the basis of information given under oath that investigating officers have a reasonable suspicion that they will find the articles they seek. Searches are not fishing expeditions. Authorised officers act on the premises that investigators have a clear understanding − by virtue of their knowledge of the investigation − of what classes of articles may have a bearing on an investigation (Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others; Zuma and Another v. the National Director of Public Prosecutions and Others, 2008). Secondly, investigators should have a clear understanding of what classes of articles are entirely irrelevant and as stated by the court in Thint (Pty) Ltd v. the National Director of Public Prosecutions and Others, Zuma and Another v. the National Director of Public Prosecutions and Others (2008), investigators should always limit their search to avoid examining irrelevant articles. The court further held that investigators are "never" entitled to simply search through everything present with the hope of finding something relevant. This is contrary to the process that is currently followed by the SAPS where "all data" of suspects are handed over to an investigation team or all data is searched with the "hope of finding something" and they are conducting "fishing expeditions" (Anon, 2016a). It is clear from the finding of the Constitutional Court which place a

restriction on investigators to limit themselves to only examine articles and containers containing or constituting classes of articles that may have a bearing on an investigation that was identified in the search and seizure warrant. If articles or classes of articles are not listed in search and seizure warrants and these articles or classes of articles are discovered on a premises, investigators will have to answer questions regarding how these articles were discovered if investigators limit their search as required by the Constitution. This does, however, not prevent investigators of discovering articles in “plain view”. If persons are investigated, for example, for making hate speech comments on Facebook, and the search and seizure warrant is sufficiently narrow-based on this transgression, investigators would be looking for evidence that a computer was used to log onto a specific Facebook profile, the Facebook profile of a user or a pseudo Facebook profile used by a user and that comments were typed on the specific computer. This information will be located by analysing the Internet history on the computer and by searching for specific remarks made by means of keyword searches. In this scenario, investigators would have no basis for accessing the calendar, Word documents, spread sheets, PowerPoint presentations or email communication of the suspect. These articles will not contain any evidence regarding the incident. Although these articles can provide circumstantial or supportive evidence, it would not have been known prior to the application and would therefore not be included in the original search and seizure warrant.

In the Ontario Court of Appeals in R. v. Jones (2011), a full bench of judges held that to test the reasonableness of a search conducted by the State should be measured against an objective-based approach. In other words, did investigators only search for information for which they had reasonable grounds or did they stray from the application of a warrant. This is in contrast with a methodology-based approach whereby the reasonableness of a search would be measured in only using keyword searches or limiting the search to only Word documents. The court held that this is an impractical approach. The court held in this case that the discovery, in plain view of evidence of child pornography was lawful, but the focus-change from that point forward to locate more evidence of child pornography was unauthorised since it did not fall within the original objective. A further illustration of this approach can be found in the Canadian case of R. v. Perkins (2013) where the investigator seized a computer on charges of theft of telecommunications and discovered child pornography. The court found that the investigator started the analysis by examining deleted space on the computer and not the active files and also did not utilise the setting of his forensic program which allows for a limitation of the data scope of the data being examined. It was found that the investigator followed search processes normally followed in child pornography investigations from the onset. It was held that his conduct was telling of his objective and the search was found to be unreasonable.

Given the magnitude of information saved on computers, it can often occur that forensic investigators discover evidence in plain view relating to other offences not specified in search and seizure warrants (Welty, 2011:10). Various mechanisms have been tried by courts to limit the discovery of information in plain view. Welty (2011:11) mentions that many courts in the United States of America have expressed the view that plain view should be limited or even eliminated with regard to digital evidence.

6.4 Summary

In this section, various identified aspects that can influence the manner in which search and seizures for digital evidence should be conducted − according to a South African legal framework − were reviewed.

These aspects include:

- The obligation to make a full disclosure in applications for search and seizure warrants.
- Search protocols and *ex ante* restrictions.
- Intelligibility.
- Overbroad seizures.
- A two-step process and off-site searches.
- The duration of seizures to create forensic duplicates and the retention of non-responsive data.
- Segregation of data.
- Privileged information.
- The searching of zones and plain view discoveries.

These impediments are discussed in the final chapter to provide a conclusion and recommendations on a proposed framework for search and seizures for digital evidence in South Africa.

CHAPTER 7 – CONCLUSION AND RECOMMENDATIONS

7. INTRODUCTION

The research study shows that aspects associated with search and seizure in general − and even more so in a digital environment − is in constant conflict with each other: the constitutional rights of suspects and the rights of the State. Any conclusions, although favouring the interest of justice, would seemingly prejudice the position of one of the parties while seemingly enhancing the position of the other. It was found to be beneficial to compare a paper environment and a digital environment when reaching conclusions. A balanced approach would be to compare the rights of the State and suspects in a traditional environment containing documents with a digital environment containing data. Neither party should be negatively impacted just because the search and seizure is a digital environment.

In this chapter, the closing remarks are discussed. Conclusions are reached, followed by recommendations and new research areas that were formed during the research process.

The conclusions are divided into two broad sections in relation to the objectives of the research study. Firstly, the conclusions on the secondary objectives are provided in relation to the use and interpretation of digital forensic-related terminology since it applies to the main objective. Secondly, conclusions on the main objective of the research study are provided in relation to the structure and execution of search and seizure warrants to obtain digital evidence in South Africa by forensic investigators. Following the conclusions, a sectional recommendation is provided for the use of digital forensic-related terminology that is fundamental for recommendations proposed in the form of a developed framework provided lastly.

7.1 Conclusions

7.1.1 Search for digital evidence

“Access” is proposed as an alternative to the concept of “search” as a more technological-orientated computer term. The proposed Cybercrimes and Cybersecurity Bill provides a definition of “access” as “to make use of, to gain entry to, to view, display, instruct, or communicate with, to store data in or retrieve data from, to copy, move, add, change, or remove data or otherwise to make use of, configure or reconfigure any resources of a computer device”. In the above-mentioned instance, the definition or interpretation provided for “access” is overbroad − specifically as an interpretation of “search”. The “access” of data is the “search” action required for forensic investigators to take notice of the content of data and to determine

whether data is relevant to the investigation and therefore covered by the search and seizure warrant while the “seize” action is the mechanism used to remove data.

It is concluded that a more accurate approach with regard to the search of digital evidence is that the creation of copies or forensic duplicates should not constitute a search action or form part of the definition of a search, since a forensic duplication process is an automated process and persons do not take notice of the content of data. The creation of a forensic duplicate should rather form part of the seize actions and the definition of “seizure”. This approach should equally apply to any other action where the content of digital documents is not exposed to persons. A practical approach − with any interpretation of the concept of “search” in relation to data – is to acknowledge that “search” actions should be divided into three distinct phases that can influence the interpretation of “search” and an “exposure-based approach” should also be taken into consideration. The first phase is the traditional process in which forensic investigators search, look for or locate physical computers on a scene. In the second phase, forensic investigators search for or segregate relevant and non-relevant information/data stored on computers. During this phase, a segregation can be done automatically whereby data is not exposed to human observation or manually whereby data is exposed to human observation. In the last phase, analyses or interpretation of only relevant data take place within the context of a larger investigation − the content is exposed to human observation.

It is supported by literature that a search of data or information only occurs when persons’ expectations of the data staying private is compromised by forensic investigators accessing that data or information by whatever means and when forensic investigators take notice of the data or information or when they observe data or information in a readable format. The following actions and terminology would apply: read, access, analyse and interpret.

For practical legal interpretation the various interpretations of “search” should be recognised and provision should be made that data can be searched in different ways in which persons take notice of content and in situations where content is still unknown to persons. Data should only be considered truly “searched” if the content is exposed to human observation. If automated searches are conducted, these searches constitute non-human examinations, scans or probes of data. In this approach, automated searches can be performed to establish whether data is responsive or unresponsive. Even private or legally privileged documents can automatically be “searched” without compromising private or legal privileges.

7.1.2 Seizure of digital evidence

Case law in South Africa dictates that “seize” means to take possession of articles and also to retain these articles. Some of the authors added that “seize” means to deprive persons of

control over seized articles. Currently, uncertainty exists within the SAPS to what constitutes "original" digital evidence. The original hard drives of the computers of suspects or the forensic duplicate records, which was created of these computers? Should the hard drives or the forensic duplicate records be seized and retained? Due to the forensic-recognised processes whereby digital evidence is collected in the form of forensically sound duplicate original records, these forensic duplicates are acceptable to judicial standards as originals. If forensic investigators, therefore, create forensic duplicates and the original hard drives are handed back to suspects, the content on these hard drives change immediately the moment suspects switch on their computers and use them. It is, therefore, concluded that forensic duplicates are the only remaining original versions of what seized computers contained at an exact point in time and forensic duplicates should be recognised as originals susceptible to seizure.

The proposed Cybercrimes and Cybersecurity Bill makes provision for "seize" by including "rendering of data inaccessible". The aspect of rendering data inaccessible is a new, but very useful concept. Subject to jurisdictional requirements, this can be a mechanism used by forensic investigators to secure online data in other jurisdictions while providing time to follow the required authorisation process for cross-border cooperation. This mechanism could allow forensic investigators to change, for example, a person's Facebook or Dropbox password in order to secure data for later retrieval and to render data inaccessible to persons.

7.1.3 Premises, containers and articles

The Electronic Communication and Transaction Act (25 of 2002) recognises the need to include digital evidence, devices and storage media in legal definitions. Various authors have recommended that the Criminal Procedure Act (51 of 1977) should be amended to include and recognise "new" digital definitions. While the new Cybercrimes and Cybersecurity Bill provides an inclusive definition for "article", the Bill does not provide a wider and more inclusive or clarifying definition for "premises", which can facilitate searches in cyberspace when no physical addresses are available.

The question regarding what premises must be defined in search and seizure warrants, being that of the suspects, the forensic investigator or the computer itself, relate to the intelligibility of search and seizure warrants − suspects and investigators should both understand precisely what search and seizure warrants authorise. South African case law recognises the need for blanket seizure of large collections of physical documents and the removal of these documents to the premises of the SAPS in certain situations without a secondary premises identified. The court also held that it is immaterial at which premises forensic duplicates are created after a seizure took place. It is, therefore, concluded that if search and seizure warrants specify that

computers can be removed from the original identified premises, then the address of a secondary premises should not influence the intelligibility of search and seizure warrants and it is, therefore, not necessary for detailed specifications of secondary premises in warrants.

In cyberspace, data is often not located in one specific area and can be distributed on servers throughout South Africa or internationally. Data can also be stored in international locations or broken up and stored in pieces in South Africa or internationally. The remote or online storage of data poses a problem to forensic investigators − prior to a search and seizure, the existence of remote or online data is unknown to them. In this situation the provisions of Section 22 of the Criminal Procedure Act (51 of 1977) can assist investigators in securing evidence without search and seizure warrants. However, in light of recent case law, courts are not in favour of warrantless search and seizures if there was sufficient time to obtain search and seizure warrants. The question, which arises, is when the police are required to seize information, which is kept in a distributed cloud environment, how the search and seizure warrant would identify the premises. It is impractical and most probably also impossible to obtain search and seizure warrants for all these premises due to the fact that data can be distributed over a number of physical servers in different jurisdictions. A possible solution is to list one of the physical locations in a search and seizure warrant and to remotely access and forensically duplicate data from the physical location listed. A second option is to list the premises of suspects and to specify the search and seizure of data not on the premises listed, but at locations under their control. This permits the remote seizure of data or as proposed by the new Cybercrimes and Cybersecurity Bill, to “render the data inaccessible. Complexities regarding jurisdictional requirements and international cross-border cooperation requests are well-documented and were not researched as part of this research project, but identified rather as a new field of study. It was found in recent case law, that the premises where forensic copies were made was immaterial as long as the premises to be searched is intelligibly defined in order for investigator and suspect to understand what is authorised in the warrant. If no physical location is available, virtual or online locations of data should be sufficient, as defined by the Electronic Communication and Transaction Act (25 of 2002) that recognises that “premises” can be defined as an “information system”.

It is, therefore, concluded that the premises of suspects or locations where data or a portion of the data is stored, should be specified and the remote seizure thereof – in line with the new Cybercrimes and Cybersecurity Bill – is permitted. If locations are unknown or cannot be determined, then locations should be specified as data stored at a location under control of suspects or the virtual or online location of data should be specified in warrants. If data is kept at a remote location and this information is unknown to forensic investigators and only discovered during a search and seizure, the data can be seized in terms of the provisions of

Section 22 of the Criminal Procedure Act (51 of 1977) without a warrant, but only if there was no opportunity to apply for a search and seizure warrant and there is a chance that suspects can destroy the data.

Both the SAPS Interim Standing Operating Procedures Dealing with Electronic Evidence (SAPS, 2016) together with the Practical Guide to Apply for Search Warrants in terms of the Provisions of Section 21 of the Criminal Procedure Act (51 of 1977), advise SAPS members to use related descriptions of articles provided in the Electronic Communication and Transaction Act (25 of 2002) listed “data”, “data message” and “information system”. Case law identifies that a wide list of items, such as inter-alia memory sticks and hard drives, upon which data can be stored is normally supplied in search and seizure warrants. Although not incorrect, no motivation could be found for this, since no requirement exists whereby a forensic investigator is required to supply an exhaustive list of the items, which will be searched through to locate the relevant article if the articles are fully described in a physical environment. This approach places a responsibility on the police to provide an exhaustive list of all items, which is sought with the risk of omitting an item. A typical example of a physical search and seizure warrant is to state that invoices, ledgers and receipts in relation to company “ABC” for the period 2001 to 2002 should be searched for and seized. In is concluded that it is appropriate to specify articles to be searched and seized, such as invoices, ledgers and receipts in relation to company “ABC” for the period 2001 to 2002 in digital form on any “data storage device”, “data processing device” and “information system”. Then all types of devices are included that can be found on a scene, such as computers, laptops and memory sticks.

7.1.4 Technically correct terms to describe data

The term “electronic” can include devices, such as clocks, radios and clock radios, and, therefore, not an exclusive term for data. “Digital” is a more technically correct term to use when describing data and can be used exclusively to refer to data.

The term “electronic” is widely used and actually forms part of the name of the Electronic Communication and Transaction Act (25 of 2002). The separation of these two terminologies is troublesome. However, it is concluded that the most accurate description for data that includes devices is the term “digital”.

7.1.5 Cellular phones versus computers

Primarily, cellular phones are described as communication devices with computing capabilities nowadays. Understandably, Canadian case law held that historically, older cellular phones were very limited and current smartphones have the same capabilities as computers. The court, therefore, includes cellular phones when computers are described. It is in part due to this ruling that it is not prudent to follow this route, since a distinction should then have to be made in every situation between old and new models of cellular phones or smartphones and this differentiation can be problematic in search and seizure warrants. It is, therefore, concluded that computers and cellular phones should be described separately and that the most elucidating collective description for computers and cellular phones is “data storage device” and/or “data processing device”.

7.1.6 Duplicate originals

Internationally, it is recognised that a digital forensic process normally starts with securing digital evidence by creating forensic copies or forensic duplicates in line with a forensic process. Forensic copies or duplicates can be validated to ensure authenticity and accuracy of digital evidence. It was found that many different terms are used to refer to the creation of forensic duplicates. The use of various terminologies was found to be technically incorrect in different situations. A forensic process should rather be described in broader generally acceptable terms to avoid judicial disputes over technical concepts when the process was correctly followed. Forensic duplicate records need to adhere to the requirements of the Electronic Communication and Transaction Act (25 of 2002). Forensic duplicates should be created in a reliable manner for evidence to be considered original. Original duplicates remain complete and unaltered and the integrity of duplicates are, therefore, intact. It was found that forensic technology has advanced to a state where duplicate originals can be created to be exact replications of originals and can, therefore, be accepted as true reflections of originals.

It is concluded that the most elucidating description, which should limit room for interpretations, is “forensically sound duplicate original records”, “forensic duplicates” or “duplicate originals”.

Forensic duplicates are subjected to stringent control and scrutiny to be scientifically proven and accepted as exact duplicates or exact versions of original data. It is concluded that forensic duplicates can be viewed as originals or duplicate originals and this also applies to any subsequent duplicates generated.

Concerns are raised concerning the description of the creation of “copies”, since copies can be perceived as not being originals, as required by the law, but South African courts are

accustomed to the creation or existence of “copies” recognised as duplicate originals, since the inception of carbon copies.

7.1.7 South African regulations

Although the Criminal Procedure Act (51 of 1977) has a longstanding reign within the legal environment of search and seizures and has been vigorously tested in countless court cases, it was established that many authors are of the opinion that this Act pre-dates data and does not cater for a digital environment explicitly. When comparing the Criminal Procedure Act (51 of 1977) with Section 19 of the Budapest Convention, authors are of the opinion that many digital-specific areas are not expressly addressed, such as digital-specific terminology, definitions, search and seizure powers and remote search and seizures. The proposed Cybercrimes and Cybersecurity Bill − if approved – will address some of these mentioned issues.

Section 14 and 15 of the Electronic Communication and Transaction Act (25 of 2002) provide the requirements for measuring digital evidence and, include originality, integrity, reliability and if data remain unchanged. The Electronic Communication and Transaction Act (25 of 2002) allows for the appointment of cyber inspectors who have specific powers. The opinion exist that it is an abnormality that the SAPS cannot utilize the procedural provisions of the Electronic Communication and Transaction Act (25 of 2002) without the assistance of cyber inspectors. In light of the power, which is bestowed upon the SAPS in terms of the SAPS Act, (68 of 1995) and the Criminal Procedure Act (51 of 1977) in terms of search and seizure, it is hard to perceive why the Police would need any procedural provisions stipulated in the Electronic Communication and Transaction Act (25 of 2002) to perform their duties or to conduct search and seizures. The value of the Electronic Communication and Transaction Act (25 of 2002) for forensic investigators lies in the fact that this Act defines cyber-crimes and provides much needed statutory requirements.

The proposed Cybercrimes and Cybersecurity Bill provides a definition of “computer”, “computer data storage device” and “computer system” as opposed to just “information system” as provided in the Electronic Communication and Transaction Act (25 of 2002). The broadening of definitions is a step in the right direction, since “information system” does not accurately describe data storage devices, such as memory sticks, data backup tapes, compact disks and all types of data storage devices. This is an aspect that is technically incorrectly addressed in the SAPS’s Practical Guide in which police members are instructed to use the description of “information system” to encompass all of the articles that can contain digital evidence. The Practical Guide refers the SAPS to the Electronic Communication and Transaction Act (25 of 2002) that provides the definition of “information system” where “information system means a

system for generating, sending, receiving, storing, displaying or otherwise processing data messages and include the Internet". The Practical Guide, however, adds the following technically incorrect interpretation: "An information system would therefore include articles commonly referred to as a … cellular telephone, flash drive, 'usb' device, compact disk and digital photograph and or video disc or card". These devices, added in applications for search and seizure warrants, should rather be defined as "data storage devices" and not "information system". A common misperception in both the Practical Guide of the SAPS and the Cybercrimes and Cybersecurity Bill, is the fact that the definition of "information system" or "computer" incorporate cellular phones. This is incorrect, and cellular phones should preferably be defined on their own or, as previously advised, as digital devices.

The definition in the proposed Cybercrimes and Cybersecurity Bill of "computer data storage device" can be limiting, since the inclusion of the word "computer" exclude many devices. "Computer" can be replaced by "data processing devices". This definition includes cellular phones, computers or any new technology not yet known. It is concluded that the inclusion of definitions of "data storage devices", "data processing devices" and "information systems" should address all requirements for identifying relevant articles.

The Cybercrimes and Cybersecurity Bill further makes provision for oral applications with regard to search and seizure warrants. It may be too early to provide an opinion, but the question is raised with the complexities of digital evidence if this proposed Section will be practical. The constitutionality of oral applications should also be considered in light of recent case law where the Supreme Court of Appeal found that a copy of the search and seizure warrant and any other documents, such as the application for the warrant, should be handed over to the suspect during a search to enable the suspect to question the validity of the search and seizure warrant if it was unlawfully issued or unlawfully executed. This ruling was also supported in recent High Court cases. If the Cybercrimes and Cybersecurity Bill is approved as is, it means that suspects can be placed in a position where they cannot defend themselves against a verbal application, unless the application is submitted in writing sooner than the proposed 48 hour period, and suspects can claim that they are denied a fair trial. In light of recent case law, courts indicated that it is not favourable to perform search and seizures without warrants. It is concluded, that search and seizures should be performed after a written application was approved and not an oral application.

7.1.8 Digital evidence as real or documentary evidence

Case law in South Africa held that digital evidence should be submitted in South African courts as real or documentary evidence and that the relevant rules of evidence should be applied

accordingly. It is not supported that the admissibility of digital evidence should be regarded as *sui generis* – in a class of its own − whereby a hybrid between traditional evidentiary rules of real evidence and documentary evidence should be applied. By following this practice, it was observed that courts only apply the validation of evidence in relation to a test of documentary evidence or real evidence and not in relation to the requirements of originality, reliability and integrity, as defined by the Electronic Communication and Transaction Act (25 of 2002).

7.1.9 Full disclosure in applications, intelligibility, overbroad search and seizure warrants, off-site searches and *ex ante* restrictions

Many of the studied doctrinal impediments are closely linked and overlap on various areas and, therefore, a collective discussion and conclusion is provided on these impediments.

The South African High Court held that a copy of the search and seizure warrant should be handed over to the suspect accompanied with a copy of the application to the search and seizure warrant. The content of applications is, therefore, of the utmost importance. Traditionally, Section 21 of the Criminal Procedure Act (Act 51 of 1977) requires applicants of search and seizure warrants to show under oath that reasonable grounds exist to believe that Section 20 articles of the Criminal Procedure Act (51 of 1977) will be located upon persons or premises. This used to be a requirement set by the State for the issuing of search and seizure warrants. With the adoption of the Constitution (1996), additional aspects were introduced and enforced by the Constitutional Court. The right of individuals to privacy and decency should be taken into consideration by authorised officers when issuing search and seizure warrants. The Supreme Court of Appeal held that applications for search and seizure warrants should be approached with circumspect and applications for search and seizure warrants should not be viewed as interdepartmental correspondence or notes. The Constitutional Court determined that authorised officers should exercise their discretion when authorising search and seizure warrants. This should be done in such a way that the rights of persons are protected as far as possible and that search and seizure warrants are not too broad and not intelligible. Overbroad search and seizure warrants are assessed by evaluating warrants and the execution of warrants. If search and seizure warrants do not specify with sufficient specificity the articles to be searched for, these warrants will be found overbroad.

Based on a study in America, it was found that authorised officers boast limited knowledge with regard to digital forensics and digital evidence. To be in a position to evaluate applications of search and seizure warrants, authorised officers require applicants to fully disclose all relevant facts to allow authorised officers to properly apply their mind. In traditional applications, applicants can satisfy these requirements by showing that reasonable grounds exist to believe

that articles in terms of Section 20 of the Criminal Procedure Act (51 of 1977) are present on a premises. Computers are a bigger risk concerning the privacy of suspects and all potential innocent individuals around them. The Canadian Supreme Court concluded that if computers are going to be searched, it should be clearly stated in applications for search and seizure warrants.

It is concluded that all relevant facts that can influence authorised officers should be stated in applications for search and seizure warrants. Relevant facts can include:

- If computers are going to be copied on a scene or if computers are going to be seized and removed off-site.
- If full system duplicate originals are going to be created.
- For how long devices is going to be seized before it is returned to their owners.
- What mechanisms are going to be followed to protect the constitutional rights of suspects.

Suspects can very easily hamper investigations when evidence is hidden, encrypted, password protected or deleted. The fact that data is intermingled on computers and data volumes are ever-increasing, law enforcement are, therefore, prevented from conducting effective searches of data on scenes. It was established that it is internationally accepted that it is impractical, not in the interest of justice and also not the least restrictive means to search computers on a scene. Internationally, it is best practice to allow law enforcement to seize physical computers containing all of the data or create forensic duplicates of all of the data stored on computers and to conduct an off-site segregation of relevant and non-relevant data. The court seemingly had no problem with permitting a search of the computers and the creation of forensic duplicates in the case of Beheersmaatscappij and Another v. The Magistrate Cape Town (2004), since the court held that the “computers could have been effectively searched and copied at the premises”. It was, however, not specified if the permitted forensic duplicates relate to the computers containing all of the data or just relevant files. Based on this remark, it is believed that if it was specified in the search and seizure warrant that the computers would have been seized and removed off-site, that full system forensic duplicates would be created, the Court would have sanctioned an off-site search. The SAPS Interim Standing Operating Procedures Dealing with Electronic Evidence (SAPS, 2016), instruct the SAPS to state on applications of search and seizure warrants if on-site or off-site copies will be made of data.

South African law should recognise a multi-step search process in which computers are searched on a scene while data is searched off-site. This process was adopted by the United

States Federal Rules of Criminal Procedure, Rule 41, Search And Seizure (2009). A multi-step process is recommended by various authors to be recognised and adopted in the legal environment of South Africa. The interest of justice is not served by attempting to search computers on a scene due to the fact that suspects can easily frustrate a search by encrypting, hiding or deleting data. It can also literally take weeks to locate data specified in search and seizure warrants. It is concluded that it should, therefore, be stated in applications for search and seizure warrants and also in subsequent search and seizure warrants that the State is permitted to seize computers containing all of the data or to create forensic duplicates and/or remove these computers off-site to create forensic duplicates. This is a practice adopted by the:

- United Kingdom (British Attorney General, 2013)
- American Federal Rules of Criminal Procedure (2009)
- Australian Crimes Act (12 of 1914)
- New Zealand Search and Surveillance Act (24 of 2012)
- Canadian Criminal Procedure and Practice, Section 490.

Although South African case law indicates that the Criminal Procedure Act (51 of 1977) does not permit the seizure and off-site search of computer containing all of the data, it is concluded that the verdict of the court was made on other defects in search and seizure warrants. If the seizure of computers containing all of the data and the off-site search thereof were the only reasons of finding warrants “unlawful, inconsistent with the Constitution and invalid”, it is strongly believed that the decision of the court could have been successfully appealed by the State on the basis that computers contain intermingled records of such quantity that computers cannot be effectively searched or data segregated on a scene. Both local and international current case law permits the blanket seizure of large collections of intermingled physical document sets if no alternative exists. It is noted that the Supreme Court of Appeal of South Africa considers the measures employed by the SAPS in sealing data and inviting suspects to be present when data is unsealed and segregated − a fair process that does not cause any prejudice to suspects.

South African case law dictates that the actions of investigators on a scene should mimic the ambit of search and seizure warrants and makes it clear what actions are permitted. As it stands without specifically addressing the issues of search and seizure of digital evidence, the actions of the forensic investigator, in seizing the computer containing all of the data, constitutes an overbroad seizure. It is, therefore, concluded that it should be stated within applications for search and seizure warrants what the practical complications are when computers are

effectively searched on a scene and it should be motivated why the seizure of computers containing all of the data or copies made of data is required. This places authorised officers in a position to apply their mind effectively with regard to constitutional requirements and to effectively authorise actions in the body of search and seizure warrants. Internationally, it is practice to use applications for search and seizure warrants to effectively obtain the approval of authorised officers for actions that are going to be executed before search and seizure warrants are issued. Clearly defined actions contribute to the intelligibility of search and seizure warrants and inform suspect about permitted actions of investigators.

It was established that with regard to the search and seizure of digital evidence, seizures normally take place before searches, but it should be highlighted that multiple steps are involved in searching digital evidence. Firstly, physical devices should be located. Secondly, the segregation of relevant and non-relevant data should take place and lastly, an analysis or interpretation of relevant data. As such, it was found that by only specifying physical devices or data in isolation, leads to overbroad seizures. It is concluded that physical devices and data should be specified in search and seizure warrants. In an informal discussion, it was determined that some unit(s) in the SAPS use two search and seizure warrants. The first is used to seize physical devices and the second search and seizure warrant is used to specify and seize data. Data or information should be specified very specifically to permit investigators to accurately identify relevant data. General terms, such as “all records” or catch-all phrases, can lead to overbroad warrants and are generally not permissible. It should be noted that within a digital environment, records can be kept in a database format and the seizure of whole databases can be required to gain access to individual records. This is already an accepted practice in a physical environment to seize whole cashbooks to gain access to individual transactions.

The opinion exists that forensic investigators should conduct pre-search previews of devices on a scene to establish whether these devices contain relevant evidence or not. Pre-search previews can be performed in a forensic sound manner by connecting computers of suspects to a write-protector device. A write-protector device allows the forensic investigators to conduct preliminary searches for specific keywords derived from a search and seizure warrant to ascertain if the content stored on computers relates to the search and seizure warrant without modifying evidence. The advantage is that a search was performed prior to the creation of forensic duplications or before data is seized. On a negative side, evidence can very easily be missed, no deleted data is recovered and password protected or encrypted files are missed. It also places a burden on the SAPS who are already experiencing a shortage in skills to conduct searches on scenes (Anon:2016a). The practical approach will be to make decisions on a case-by-case basis without making it mandatory, which is in line with current case law that makes provision for the forensic investigators to view physical file labels of files to decide whether

these files possibly contain relevant information and to determine if a more in-depth review is needed to confirm the presence of evidence. If pre-search previews are done and no evidence is found due to possible constraints, such as data deletion and encryption, investigators can still seize computers to complete more in-depth searches to ascertain that computers do not contain evidence.

Various mixed opinions exist regarding *ex ante* restrictions set by international courts and authors. In the area of conducting searches at the premises of lawyers, courts are more inclined to require procedures to limit the potential of overbroad searches, which can expose legally privileged information. It was held by the South African Constitutional Court that in these situations, extra care should apply. The Constitutional Court determined that authorised officers should exercise their discretion to authorise search and seizure warrants in such a way that the rights of persons are protected as far as possible and that search and seizure warrants are not too broad and warrants should be sufficiently intelligible. Authorised officers have the right to scrutinise the structure of search and seizure warrants to ensure that warrants are structured to protect the rights of suspects as far as possible. It was, however, found that although it is in the power of authorised officers to approve or decline applications for search and seizure warrants, it is not practice to specify *ex ante* requirements. Emphasis should be placed on *ex post facto* evaluations of the content of search and seizure warrants and the execution thereof. It was found in case law that mechanisms employed by the SAPS during the execution of search and seizure warrants to protect the rights of suspects and privilege data, resulted in courts upholding search and seizures. Internationally, opinions were found where it is required by law enforcement to set out if authorised officers permit over seizures of computers containing all of the data, how the analyses of data will be managed to protect the rights of suspects and how the least restrictive means will be followed to serve the purpose. Some of these measures include search criteria in which keywords are specified or independent filter teams are used to segregate relevant and non-relevant data and they only hand over relevant data to forensic investigators. Although the majority opinion is that authorised officers are not technically knowledgeable enough to set *ex ante* restrictions and should not prescribe the State on how to conduct investigations, the approach followed by the Canadian Supreme Court is supported − in some cases it is more prudent to set or require *ex ante* restrictions, especially in situations where law firms or sensitive investigations are conducted.

In the majority of cases, computers pose technical complexities and it is not feasible to search data on a scene. Forensic duplicates will have to be created of computers containing all of the data. If the creation of full system forensic duplicates are not permitted, the State is placed in an unattainable position and would not be in a position to conduct digital forensic investigations. If digital forensic experts are only permitted to forensically duplicate and analyse limited files,

digital forensic experts would not be placed in a position to place evidence in context. To place evidence in context, includes the ability to investigate all of the elements of a crime in relation to evidence not imbedded within files but rather located in system files or elsewhere on computers, to verify or dispute versions placed before them during testimonies and maybe most importantly, to investigate any evidence pointing away from the guilt of suspects.

It is concluded that due to these practical constraints and in serving the interest of justice, overbroad seizures of computers should be permitted as a method to secure evidence, but not as a blanket approval to investigate all of the data on computers unrestrictedly and off-site. If this was permitted, suspects would not be in a position to invoke their right to immediately oppose the seizure of non-relevant data, based on the ground that there is no other option for the State but to seize computers containing all of the data. In effect, digital forensics are requesting courts to permit overbroad seizures, since it is the only route that serves the interest of justice, but it seemingly requires suspects to postpone their right to immediately invoke their constitutional rights.

The only way to guard against this leniency towards seizing the computer containing all the data becoming the norm for overbroad seizures is to employ mechanisms to manage the review of data. Forensic investigators, should be permitted, just as on a normal crime scene to review all files, following various mechanisms structured around an approach of first following least intrusive means with the objective of first and foremost segregating relevant and non-relevant files. This is proposed as a mandatory step, since the alternative would result in forensic investigators having continual unrestricted access to a “digital scene” for the duration of an investigation, which can be months or even years. It is proposed that forensic investigators should segregate relevant and non-relevant data to allow suspects to protect their rights or to show that forensic investigators did not stray outside the ambit of warrants.

Suspects are permitted to be present when physical searches are performed at their premises. Suspects should also be afforded the opportunity to be present when data is segregated. However, the presence of suspects during data segregation is not a requirement. It may be impractical to have hundreds of suspects present during the segregation of data, especially if this happens over long periods of time.

It is concluded that the proposed second alternative is more practical − the use of independent filter teams. This practice was successfully applied by the Competition Commission of South Africa. Relevant and non-relevant data can be segregated without suspects being present, but suspects and the court were placed in a position to audit or review the process. Specialised skills and equipment are required to search through data. It is envisaged that digital forensic investigators should perform the segregation of relevant and non-relevant information.

Independent filter teams can be digital forensic investigators within the SAPS or can operate as external teams. Digital forensic investigators should use applications for search and seizure warrants as the only ambit to identify relevant and non-relevant files. The British Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners provide a good structure in which the actions of filter teams are monitored. These guidelines specify that lead investigators should develop a strategy on how the data should be analysed. If forensic tools are used to sift through data, suspects should be supplied with a list of search terms. A detailed record should be made of the strategy used and the analytical techniques used to segregate data. The record should include the names of the persons who carried out the process and what keywords were used on the specified dates and times. It is advised that digital forensic investigators should firstly consider the most obvious route to locate evidence, but they should not be restricted from expanding the parameters of their analysis. It is not advised that keywords should be viewed as the only mechanism to search data, since many files are not responsive to keywords alone. The actions of digital forensic investigators are susceptible to cross-examinations to determine if the search methodology was aimed at only discovering information relevant to a search and seizure. All of the actions performed by digital forensic investigators should, therefore, be recorded as specified as stipulated by the British Auditor General and required by the ISO 27037 and 27043 Standards. This will allow suspects who are not present to determine if the search through data was performed within the ambit of the search and seizure warrant. From an unstructured interview, it was established that the Competition Commission of South Africa does not provide individuals with a list of keywords used to locate relevant information. This is done to prevent individuals of discovering too much information regarding an investigation. In light of recent criminal law cases where the court held that a copy of the application for the search and seizure warrant should be handed with the search and seizure warrant to suspects, the approach by the Competition Commission of South Africa.to withhold the keywords from the respondent may be found to be irregular.§

Following the segregation of data, digital forensic investigators can then release all of the relevant information to forensic investigators for an analysis and investigation. If additional information outside of the original search and seizure warrant is required by forensic investigators, and a new search needs to be conducted, a new search and seizure warrant should be applied for. The same route is followed on a crime scene. By retaining original forensic duplicates, digital forensic investigators are in a position to place any evidence in context by having access to system files and registry files and they can explore any version placed on record by suspects.

Including this approach in applications and search and seizure warrants, contributes towards protecting the constitutional rights of suspects. It also ensures that forensic investigators stay

within the ambit of warrants, although the overbroad seizure of computers containing all of all data is permitted.

7.1.10 Duration of seizures to create forensic duplicates and retention of non-responsive data

The Criminal Procedure Act (51 of 1977) regulates the right of the State to retain or return seized articles. There is, however, no specific period in days provided. When computers are seized from suspects and the computers are stolen articles or contain illegal material, such as child pornography, the Criminal Procedure Act (51 of 1977) is clear that these computers should be forfeited to the State or returned to the rightful owner. If computers are seized and after the investigation it is established that these computers do not contain any evidence, the Criminal Procedure Act (51 of 1977) stipulates that these computers should be returned. The difficulty is with computers, which contains both relevant and non-relevant information as well as determining if it would be feasible to specify a specific period in days in terms of which computers must be forensically duplicated and returned.

The Australian Crimes Act (12 of 1914) provides that forensic investigators should create forensic duplicates of computers and return computers within 14 days or they should apply for an extension. The retention period of the SAPS is estimated at two months while the DPCI is between two weeks to two months. The retention period for cellular phones is between one to two weeks. It has to be born in mind that at this point in time, persons are not guilty of an offence and can actually be innocent. If the computers of a business are seized and returned weeks or even months later, it is detrimental to the business and can cause financial ruin – even if the business is innocent. In a paper environment, suspects may, therefore, retain a copy of the search and seizure warrant. People are also very reluctant to relinquish their cellular phones if they are unable to communicate freely for an extended period of time. During an unstructured interview (Anon, 2016a), it was established that it is the norm of forensic investigators to conduct search and seizures without digital forensic investigators available to create forensic duplicates on a scene. A blanket seizure of all devices, where the data was the object of the search and seizure, has therefore become the norm and not the exception, whereas it should only be considered if digital forensic investigators are not available or the search and seizure operation cannot be rescheduled. As was stated in case law, applications for search and seizure warrants should not become a mere formality and the exclusion of digital forensic investigators on a scene should not become the norm. A search and seizure should only be performed without a digital forensic investigator in cases when one is not available and the search and seizure cannot be scheduled accordingly. As was commented in the case of Beheersmaatscappij and Another v. The Magistrate Cape Town (2004), the fact that the State

may not have the capacity should not validate the unnecessary infringement of the rights of a suspect rights by becoming the standard way of performing digital search and seizures.

It is concluded that this period of retaining devices to create forensic duplicates should be as short as possible, since forensic duplicates are acceptable as originals and the retention of originals is not required. It is preferable that a forensic duplicate is created on a scene if possible, and original devices should only be seized if no digital forensic investigator is available to attend to the search and seizure or if too many devices are seized on a scene. It is advisable that cellular phones should be prioritised due to the perception of privacy concerns associated with them and the need of access to communication by suspects. The period of retention of devices to facilitate the creation of a forensic duplicate does not need not be extensive due to the fact that the SAPS have a number of units specialising in digital forensic investigations situated in main areas throughout South Africa. This information was shared during an unstructured interview (Anon, 2016a). The DPCI created a triage team to expedite the turnaround time on cellular phones − the creation of forensic duplicates of all devices should, therefore, also be a priority and should happen expediently.

The British Attorney General (2013) provides that in cases where relevant and non-relevant information is inextricably linked and the removal of non-relevant information can prejudice the use of relevant material, the retention of both the relevant and non-relevant material is permitted. It is, however, specified that forensic investigators may not stray into non-relevant information during subsequent investigations. This emphasises the importance of a primary phase of identifying relevant and non-relevant information prior to an analysis of data, which is strongly supported.

A number of options are available to address the importance of a primary phase of segregating relevant and non-relevant data. Digital forensic investigators can conduct a comprehensive search after data recovery was performed to identify relevant files with associated information, such as metadata, located in other locations or system files. Associated information can be exported as a new forensic duplicate and can be forensically validated. This procedure results in a second forensic duplicate containing only relevant information and associated information. The original forensic duplicate containing relevant and non-relevant information can then be destroyed or handed over to the suspect. Unfortunately, the workload of digital forensic investigators are doubled and the destruction of original copies can be found to be prejudiced at a later stage. Digital forensic investigators are under a tremendous risk to identify all of the related and associated information this early in an investigation and can be detrimental when prosecution occurs. It is also costly to the State due to the fact that two hard drives are used. A second option is to use digital forensic investigators as independent filter teams, as already discussed. It would be the task of the filter team to segregate relevant and non-relevant

information based on the search and seizure warrant. This will permit that only relevant information is exposed to the forensic investigator while limiting the digital forensic investigator from further accessing inextricable linked material which may not be examined further, forensically duplicated or used for any purpose other than validating the integrity of the relevant material.

In 2007, the court expressed the opinion that it is satisfied that the seizure of computers containing all of the data was not overbroad due to the fact that the digital forensic investigator − at that stage − acted as an independent filter team and only handed data that fell inside the ambit of the search and seizure warrant to the forensic investigator. If this procedure is compared with the current practice of the SAPS, established during an unstructured interview (Anon, 2016a), no segregation of data is performed. All of the data found on computers are handed to forensic investigators. It is concluded that while overbroad seizures of computers should be permitted, the seizure of data, as a result of the manner in which all of the data was exposed to forensic investigators, results in an overbroad seizure of data. The interviewee expressed the opinion that forensic investigators do not know what they are looking for in terms of digital evidence and they usually go out on a “fishing expedition”, which is nothing more than an overbroad and unsanctioned seizure.

It is concluded that when relevant and non-relevant information is inextricably linked – in literally all digital investigations − both the relevant and non-relevant material should be retained. However, forensic investigators should not obtain access to all of the data and non-relevant information may only be accessed for the purpose of validating associated information in relation to relevant information. It is advised that the original forensic duplicate should be retained and subsequent copies should be created which contain only relevant data. An independent filter team should be used to conduct the segregation of relevant and non-relevant data.

7.1.11 Privileged information

South Africa distinguishes between matrimonial privileged and legally privileged information. Although case law recognises that privileged information may not be seized, but sealed and kept separate – this cannot happen when computers are seized. Once a forensic duplicate is created of digital evidence, no piece of the data can be removed from the forensic duplicate. If suspects are given the opportunity to delete information from their computers, forensic tools at the disposal of the State can very easily recover deleted data and data previously deleted on a hard drive. Similarly, suspects could have deleted privileged information prior to a seizure and their computer can, therefore, contain no active privileged information at the time of a seizure. If

the SAPS perform data recovery, deleted privileged information is recovered or if a keyword is run, deleted information is retrieved. It is, therefore, impractical for persons to identify privileged information in only active data before a data recovery has been done. This means that privileged information can only be identified practically after the SAPS have seized data and data was pre-processed for an analysis or when data recovery was performed.

The practical complication of digital evidence is that if all of the data on computers are forensically duplicated and forensic duplicates contain privileged information that was sealed due to a claim of privileged information by suspects, at some stage in an investigation the forensic duplicate must be unsealed to access the non-privileged data because otherwise the whole forensic duplicates become unusable to the State.

It is acknowledged that only relevant information can be forensically duplicated on a scene, excluding the privileged data, but due to the risks with regard to the interest of justice, as was already discussed, it is not advised. The only practical conclusion reached is that computers containing all of the data − including privileged data – should be copied and independent filter teams should filter out privileged data identified by suspects. If suspects are unable to identify privileged information, they can supply independent filter teams with keywords to facilitate and expedite this process or generic keywords can also be used. If suspects do not identify any privileged information, independent filter teams can identify potentially privileged information if it is encountered. Suspects can be given the opportunity to identify privileged information prior to data recovery. However, it is advised that this should be done after data recovery was performed.

7.1.12 Searching of zones and plain view discoveries

On physical scenes, forensic investigators can restrict or focus their investigation on specific zones or areas in line with the type of articles being searched for. In digital searches, this can be problematic, since the size of data is irrelevant and files can be stored in many formats. It was determined that various mechanisms can be employed to restrict the discovery of non-related information, but a risk will always exist during digital investigations that non-relevant information is accessed or other evidence is discovered in plain view.

In a paper environment, forensic investigators are only permitted to seize relevant information listed in an original search and seizure warrant. If articles are discovered on a scene in plain view, these articles can be seized or handled in terms of the provisions of Section 22 of the Criminal Procedure Act (51 of 1977) or a new search and seizure warrant can be applied for. If only relevant documentary information is seized, and forensic investigators discover evidence off-site regarding another crime, they are not in a position to return to an original scene to

further a new investigation without a new search and seizure warrant. If the seizure of computers containing all of the data is permitted, forensic investigators are not permitted to repeatedly search these computers with the purpose to discover new evidence that falls outside the original search and seizure warrant.

It is concluded that by making use of independent filter teams and following the process already discussed of first searching in the most obvious locations, digital forensic investigators should experience no problem defending the discovery of additional evidence found in plain view. If digital forensic investigators discover information in plain view, it is advised that a search and seizure warrant should be obtained after initial discoveries were made to extend a search to locate more evidence relating to the new suspected offences.

7.2 Recommendations

The following recommendations are provided based on the research done. Recommendations are provided in a structured and chronological fashion in line with the different phases on how search and seizure warrants are applied for, structured and executed. A level of overlapping exists due to the close proximity of aspects between areas. Some of these recommendations apply to a number or all of these phases while others apply to only one phase. Recommendations are provided according to the following structure:

- General recommendations
- Terminology recommendations
- Recommendations on a proposed framework
    - Application for a search and seizure warrant
    - A search and seizure warrant
    - Execution of a search and seizure warrant

7.2.1 General recommendations

- Forensic investigators and judiciary should be adequately trained in digital forensics and digital evidence to fully understand the technical complexities that digital evidence pose to legislation and to be able to effectively draft and execute search and seizure warrants for digital evidence in an intelligible manner.
- Digital forensic investigators should be involved in the drafting of applications for search and seizures warrants for digital evidence setting out the complexities and

grounds why a required framework must be followed, based on their unique skills, qualifications and experience.

- Oral applications for search and seizure warrants for digital evidence should not be used and the practice of utilising written applications for search and seizure warrants should be continued.

- *Ex ante* restrictions should not be placed by authorised officers on forensic investigators by including restrictions in search and seizure warrants.

- The seizure of computers containing all of the data and an off-site search should be permitted.

- The subsequent premises of the forensic investigators, where forensic duplicates are created, should not be stated in search and seizure warrants as a separate premises.

- The forensic investigators should be allowed to seize computers for only a specific period to allow for the creation of forensic duplicates. If this period is exceeded, an application for the extension of the seizure of these articles should be brought before the court.

- A distinction should be made between the period in which computers must be returned and the period in which cellular phones must be returned due to the impairment of communication of persons.

- It is recommended that similar legislation as the Australian Crimes Act (12 of 1914) Section 3LB and the New Zealand Search and Surveillance Act (24 of 2012) Section 111 should be included within the Criminal Procedure Act (51 of 1977) for remote search and seizures in South Africa or elsewhere.

- Forensic sound duplicate original records or forensic duplicates should be recognised as originals and are susceptible to seizure and the original hard drive of a suspect need not be retained unless it is defined as an article or contains data, which may not be legally possessed.

- The practice of obtaining two search and seizure warrants, one setting out the physical premises and the physical devices to be seized, and the second setting out the computers on a premises and the data as the articles to be seized, should not be followed.

- In determining if data was searched, it should be assessed whether the content of the data was, and to what extent, exposed to human observation.

- In submitting documentary or real evidence originating from originally seized digital evidence, the evidence should also be assessed in terms of originality, reliability and integrity, as defined by the Electronic Communication and Transaction Act (25 of 2002).

7.2.2 Terminology recommendations

The following recommendations are made in relation to the correct use of terminology within a framework for applications and in search and seizure warrants for digital evidence by forensic investigators in South Africa:

- The term “digital” should be adopted and used instead of “electronic” or “cyber”.

- The Cybercrimes and Cybersecurity Bill should be amended to exclude “copy” as part of the definition of “access”, but should rather be used as part of the definition of “seize”.

- The definition of “search” and “seizure of data” should stay two separate indistinguishable actions.

- The three distinct phases of “search” should be recognised and used appropriately, namely: the location of data containing devices, the segregation of relevant and non-relevant data, and the analysis or interpretation of relevant data.

- The definition of “seizure of data” in the new Cybercrimes and Cybersecurity Bill, which includes “the rendering of data inaccessible”, should be recognised as a means of seizure.

- The definition in the proposed Cybercrimes and Cybersecurity Bill of “computer data storage device” should be limited to only refer to “data storage device”.

- The description of “computer” cannot be all inclusive of all devices that can store, process and transmit data. Cellular phones should be defined separately.

- The terms “data storage device” and “data processing device” are more accurate collective terms for cellular phones, computers and other devices that can store, process and transmit data.

- The most elucidating description, which should limit room for interpretation, is the creation of a “forensically sound duplicate original record” or a shortened version “forensic duplicate” or “duplicate original”.

7.2.3 Recommendations for a proposed framework

It is recommended that the following framework should be followed by forensic investigators during the search and seizure of digital evidence in South Africa:

7.2.3.1 Application for a search and seizure warrant

Although the application of a search and seizure warrant and the search and seizure warrant itself are two separate documents, these two documents are inseparable and both should be handed together to suspects, according to case law.

- The application of a search and seizure warrant should be integrated in a search and seizure warrant, namely: “As per information provided to me under oath, as described in Annexure X, with Annexure X being the application of the search and seizure warrant”.

- To assist authorised officials in fully applying their mind, applicants for search and seizure warrants should disclose all of the relevant facts, such as the computers that will be seized and removed off-site where a full system duplicate original will be created or if a duplicate original will be created onsite. The reasons why this is needed should be stated in an application.

- It should be stated if a digital forensic investigator will be on a scene and if a forensic duplicate will be created on a scene.

- If it is required to seize devices and remove them from a scene, it should be specified for how long these devices are going to be retained before a forensic duplicate is created and the original returned to suspects.

- Forensic investigators should include the mechanisms they will employ to protect the constitutional rights of suspects or to stay in the ambit of search and seizure warrants in the application of search and seizure warrants. By implication of current case law, this will inadvertently become part of the execution of search and seizure warrants allowing suspects to enforce their rights at an early stage of an investigation. Authorised officers do not have to specify mechanisms, but the

forensic investigators do specify mechanisms in applications, which does not result in *ex ante* restrictions. These mechanisms should include:

- Suspects may be present when relevant and non-relevant data is segregated.
- The segregation of relevant and non-relevant data is a mandatory step.
- An independent filter team should be used to segregate relevant and non-relevant data.
- An independent filter team should be limited to search only for data defined in a search and seizure warrant and should not adhere to external requests from a forensic investigator.
- An independent filter team should document all of the search actions taken to such a detailed extent that suspects and the court are able to scrutinise the actions to determine whether these actions fell within the authorisation of the search and seizure warrant.
- Only relevant information identified by an independent filter team should be handed to a forensic investigator for investigation.
- If information of another crime is discovered in plain view, a second search and seizure warrant should be obtained.
- If it is suspected that data is kept off-site in an online storage space, it should be stated that this information can be destroyed by suspects and that the data should be seized remotely in terms of the provisions of Section 22 of the Criminal Procedure Act (51 of 1977) or rendered inaccessible in terms of the provisions of the new Cybercrimes and Cybersecurity Bill.
- If it is suspected that data is kept off-site in an online storage space, suspects should be requested by a search and seizure warrant to identify the location of such storage space and/or to supply the password for access to such storage space.
- If it is suspected that data is kept off-site in an online storage space, a digital forensic investigator, who is competent and qualified to secure such data remotely, should be present on a scene and should be responsible for the collection or securing of this data.

- A statement of a digital forensic investigator setting out the technical requirements and aspects should be attached as an annexure to a search and seizure warrant.

7.2.3.2 Search and seizure warrants

A search and seizure warrant should include/specify:

- The heading namely; Search and seizure warrant in terms of the provisions of sections 20 and 21 of the Criminal Procedure Act (51 of 1977);
- Articles in terms of Section 20 of the Criminal Procedure Act (51 of 1977) that should be searched for.
- The investigator as a police official, who will be in charge of the search and seizure. The name, rank and service number of the investigator should be provided and the details of the police official, including the digital forensic investigator(s) who will assist the investigator and attend to the search and seizure.
- A complete description of the premises.
- The crime being investigated as set out in legislation.
- Both the physical device and the data which is relevant.
- The data to be searched for with sufficient clarity. General or “catch-all” phrases, such as “all records” and “any and all records, but not limited to” should not be used.
- A description of the articles by providing a detailed description, such as child pornography, invoices of company “ABC” in the form of data records, data messages on/in “data storage device”, “data processing devices” and “information systems”.
- Suspicions of data kept off-site in an online storage space. Suspects should be requested in the search and seizure warrant to identify the location of such storage and/or to supply the password for access to such storage space.
- Intelligible content. Care should be taken to keep the content free of technical jargon.

7.2.3.3 Execution of search and seizure warrants

- Search and seizures should be executed after obtaining a search and seizure warrant and warrantless search and seizures − where obtaining a search and seizure warrant defeats the purpose – should only be performed if there is no time available to obtain a search and seizure warrant.
- The investigator identified in the search and seizure warrant should be present.

- A digital forensic investigator should be present on a scene to create forensic duplicates on the scene. Only in exceptional cases should devices be seized and removed or where a digital forensic investigator is not available or the search and seizure operation cannot be scheduled when a digital forensic investigator is available.

- A three step search process is proposed:

    - Step one − Location of data containing devices

        - A forensic investigator is responsible for locating and identifying all “data storage devices”, “data processing devices” and “information systems”.
        - These devices should be pointed out by the forensic investigator to the digital forensic investigator.
        - If a digital forensic investigator is not available on a scene, the forensic investigator should seize and seal computers containing all of the data for further investigation by a digital forensic investigator.

        - If a digital forensic investigator is available on a scene:

            - It is advisable that a pre-search preview should be performed, but it is not a requirement. Pre-search previews should only be performed in a forensically sound manner by competent digital forensic investigators. Even if a pre-search preview is done and no evidence is found, an investigator may still need to seize the computers to perform a more comprehensive assessment due to aspects, such as encryption and deletion. A pre-search preview also establishes if data is kept off-site in an online storage space.
            - If data is kept off-site in an online storage space, the data should be secured by means of a remote seizure or by rendering the data inaccessible.
            - To secure evidence, a forensically sound duplicate original record should be created of the computer containing all of the data and seized.
            - If forensic duplicates are not created on a scene, these duplicates should be created within a reasonable time or at a specified time.

- Step two − Segregation of relevant and non-relevant data
    - If the seizure of computers containing all of the data is permitted, an independent filter team should be used. The segregation of relevant and non-relevant data should be a mandatory step.
    - The independent filter team should be permitted to retain full forensic duplicates to be able to place evidence in context, for reporting purposes on relevant information or for testimonial purposes. Subsequent investigations may not touch non-relevant information.
    - Suspects may be present when relevant and non-relevant data is segregated, but it is not a mandatory measure.
    - All of the required steps to prepare data for an investigation should be followed, including data recovery and the indexing of data.
    - Suspects should be afforded an opportunity to identify privileged data after a data recovery was performed or after relevant data was identified. Even in cases where privileged information is not claimed, a digital forensic investigator should focus on preventing privileged material from being handed to a forensic investigator. Any privileged information should be separated from relevant data and should be submitted to an authorised independent party for review.
    - An independent filter team should construct an investigation plan or an analysis plan to highlight the location of relevant information at the most obvious location or high-potential places. An investigation can then be expanded to include less likely places.
    - All of the actions taken to locate relevant information by an independent filter team should be well-documented in detail to allow suspects or a court to scrutinise their actions. Actions can include the setting out of an analysis strategy, what search parameters and/or keywords were used and who performed what analytical actions on what date.
    - An independent filter team should be limited to searching for data as defined in a search and seizure warrant and should not adhere to external requests from a forensic investigator.
    - Only relevant information identified by an independent filter team may be handed to a forensic investigator for investigation.
    - If additional evidence is discovered in plain view, which falls outside the original search and seizure warrant, further searches into more

evidence in this regard should only be conducted after a new search and seizure warrant was obtained.

- Step three − Analysis or interpretation of relevant data
    - Once a forensic investigator receives a copy of the relevant information from a digital forensic investigator, the forensic investigator can conduct an investigation and an analysis of the data.
    - A forensic investigator can request the digital forensic investigator to widen the scope of a search for data, but only if it falls inside the ambit of the original search and seizure warrant.
    - If information is required, which falls outside the original search and seizure warrant, and if additional evidence is discovered in plain view, which falls outside the original search and seizure warrant, a new search and seizure warrant should be obtained.
    - In cases where no evidence is located on devices, forensic duplicates should be returned or destroyed.
    - If suspects are found not guilty, and the State is not going to appeal the verdict, forensic duplicates should be destroyed or returned.

7.3 Further identified fields of research

The following areas emanated from this study and have been identified as fields for further research:

- The new Cybercrimes and Cybersecurity Bill makes provision for rendering data inaccessible. This can be applied to secure or seize data in other jurisdictions and should be researched in relation to jurisdictions and mutual legal assistance requests.

- It is recommended that research should be conducted on how South African courts should consider the requirements of Section 14 and 15 of the Electronic Communication and Transaction Act (25 of 2002) in relation to the Rules of Evidence of Documentary and Real Evidence.

- Acceptable or practical durations, which the forensic investigators require to retain devices to be able to create forensic duplicates, should be researched.

- Jurisdictional requirements for remote search and seizures should be researched.

7.4 Summary

The hypothesis was confirmed that it is possible to develop a framework for search and seizure warrants for digital evidence, which contains the correct terminology and sets out the correct application and structure for search and seizure warrants for digital evidence for forensic investigators in South Africa.

It was established that the seizure of computers containing all of the data should be permitted due to the unique complexities associated with computers in relation to search and seizures for digital evidence, such as intermingled documents, encryption, data sizes and privileged information. Overbroad seizures should be motivated by means of a comprehensive application setting out the grounds upon which an overbroad seizure should be permitted. This will place authorised officers in a position to apply their mind and to evaluate if sufficient grounds exist to permit the required infringement on the rights of suspects. An application should show that although an overbroad seizure is permitted, resolute measures will be employed to ensure that the forensic investigator will not gain access to more data than what he/she is authorised to in terms of the search and seizure warrant and that the constitutional rights of suspects in South Africa can be enforced and protected − in a digital environment and in a physical environment.

The importance of self-restraint, self-regulation and the true spirit, purports and objectives of the South African Constitution (1996) is truly tested in the environment of search and seizures for digital evidence and the importance of a quote from William Pitt (1763) is again emphasised:

> *The poorest man may, in his cottage, bid defiance to all the force of the Crown. It may be frail; its roof may shake; the wind may blow through it; the storm may enter; the rain may enter; but the King of England may not enter; all his force dares not cross the threshold of the ruined tenement.*

Although it was established that in very few cases in South Africa the technical aspects was argued in detail, it was found that the majority of conclusions are astute. This is the advantage of case law since knowledge can change old perception and shape new direction. Some may feel that the findings of this research study can frustrate and complicate search and seizures for digital evidence. However it is hoped that the readers realises that this study attempted to improve and strengthen the methodology used by forensic investigators and to assist in building concrete cases against suspects. It is trusted that this research study supports a better understanding of search and seizures for digital evidence and serves as a basis for promoting healthy arguments to further refine the South African legal environment.

REFERENCE LIST

Acts ***see*** Australia, Canada, South Africa, United Kingdom & United States of America.

American Academy of Forensic Sciences. 2008. AAFS digital & multimedia sciences. http://www.aafs.org/students/choosing-a-career/types-of-forensic-scientists-disciplines-of-aafs/ Date of access: 5 Jan. 2016.

Angermeier, V. 2010. Swinging for the fences: How Comprehensive drug testing inc missed the ball on digital searches. *Journal of Criminal Law and Criminology*, 100(4):1598 & 1615.

Anon. 2016a. Current policy and procedure on digital search and seizure by the SAPS [telephonic interview]. 15 Sept., Pretoria.

Anon. 2016b. Current policy and procedure on digital search and seizure by the Competition Commission of South Africa [personal interview]. 17 Oct., Pretoria.

Association of Chief Police Officers. 1997. Good Practice Guide for Computer-Based Electronic Evidence version 5. http://www.digital-detective.net/digital-forensics-documents/ACPO_Good_Practice_Guide_for_Digital_Evidence_v5.pdf Date of access: 27 Dec. 2015.

Australia. 1914. Australian Crimes Act 12 of 1914.

Ball, C. 2002. Computer forensics for lawyers who can't set the clock on their VCR. http://www.craigball.com/_OFFLINE/cf_vcr.pdf Date of access: 12 May. 2016.

Ball, C. 2011. Beyond data about data: The litigator's guide to metadata. http://www.craigball.com/metadataguide2011.pdf Date of access: 1 Nov. 2015.

Bartholomew, P. 2014. Seize first, search later: The hunt for digital evidence. http://digitalcommons.tourolaw.edu/cgi/viewcontent.cgi?article=2570&context=lawreview Date of access: 10 Aug. 2016.

Basdeo,V. 2009. Constitutional perspective of police powers of search and seizure in the criminal justice system. Pretoria: UNISA. (Thesis-Masters).

Basdeo, V. 2012a. Constitutional challenges to warrantless searches. *African Journal of International and Comparative Law*, 20(2):164.

Basdeo, V. 2012b. The legal challenges of search and seizure of electronic evidence in South African criminal procedure: A comparative analysis. *South African Journal of Criminal Justice*, 25(2):198-211.

Binary Translator. (2016). http://binarytranslator.com Date of access: 10 Aug. 2016.

Bouwer, G.P. 2014. Search and seizure of electronic evidence: Division of the traditional one-step process into a new two-step process in a South African context. *South African Journal of Criminal Justice*, 27(2):156-171.

Brenner, S.W. & Fredericksen, B.A. 2002. Computer Searches and Seizures: Some Unresolved Issues. *Michigan Telecommunications and Technology Law Review*, 8(1):82.

British Attorney General's Guidelines on Disclosure: Supplementary Guidelines on Digitally Stored Material. 2011. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/16239/Attorney_General_s_guidelines_on_disclosure_2011.pdf Date of access: 5 Jan. 2016.

British Attorney General's Guidelines on Disclosure for Investigators, Prosecutors and Defence Practitioners. 2013. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262994/AG_Disclosure_Guidelines_-_December_2013.pdf. Date of access: 10 Aug. 2016.

Brown, C.L.T. 2010. Computer evidence: Collection and preservation. 2nd ed. Hingham, Massachusetts: Charles River Media, Inc.

Canada. 1982. Constitution Act, 1982.

Canada. 2002. Lavallee, Rackel & Heintz v. Canada (Attorney General) 2002 (3) S.C.R. 209.

Canada. 2002. R v. Munshi 2002 CanLII 39110 (ON SC).

Canada. 2011. R. v. Jones 2011 ONCA 632.

Canada. 2013. R v. Tyler Perkins 2013 ONSC 1807.

Canada. 2013. R v. Vu 2013 S.C.J. No. 60, 2013 (3) S.C.R. 657, at para. 22 (S.C.C.).

Casey, E., ed. 2000. Handbook of computer crime: Forensic tools and technology. London: Academic Press.

Casey, E., ed. 2011. Digital evidence and computer crime: Forensics science, computers and the Internet. 3rd ed. Amsterdam: Elsevier Academic Press.

Caloyannides, M. A. 2003. Digital "evidence" and reasonable doubt. *IEEE Security and Privacy*, 1(6):89-91.

Chan, G. 2014. Life after Vu. *Supreme Court Law Review*, 67(2):442.

Chisum, W.J. & Turvey, B. 2000. Evidence dynamic: Locard's exchange principle Crime Reconstruction. *Journal of Behavioural Profiling*, 1(6):89-91.

Christensson, P. 2005. What is the difference between analog and digital technology? http://pc.net/helpcenter/answers/difference_between_analog_and_digital Date of access: 10 Dec. 2015.

Clark, K. & Connolly, M. 2006. A guide to reading, interpreting and applying statutes. https://www.law.georgetown.edu/academics/academic-programs/legal-writing-scholarship/writing-center/upload/statutoryinterpretation.pdf Date of access: 15 Feb. 2016.

Cole, K.A., Gupta, S., Gurugubelli, D. & Rogers, M.K. 2015. Review of recent case law relating to digital forensics: The current issues. 2015 Conference on Digital Forensics, Security and Law, Daytona Beach, Florida. p.96.

Constitution ***see*** South Africa.

Cornell University Law School. n.d. The Committee Notes on Rules – 2009 Amendment to the rule change. https://www.law.cornell.edu/rules/frcp/rule_15 Date of access: 17 Jul 2016.

Council of Europe. 1995. Recommendation No. R (95) 13 of the committee of ministers to member states concerning problems of criminal procedural law connected information technology. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76 Date of access: 10 Nov. 2015.

Council of Europe. 2001a. Cybercrime Convention Budapest. http://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 Date of access: 29 Apr. 2016.

Council of Europe. 2001b. Explanatory Report to the Convention on Cybercrime. http://www.oas.org/juridico/english/cyb_pry_coe.pdf Date of access: 29 Apr. 2016.

Couzyn, Hertzog & Horak. n.d. https://www.hg.org/article.asp?id=5351 Date of access: 16 Jul. 2016.

Craiger, J.P. & Shenoi, S. 2007. Advances in digital forensics III. Boston: Springer.

Cross, M. 2008. Scene of the cybercrime. 2nd ed. Arlington: Syngress Publishing.

Digital Intelligence. 2016. Forensic Duplicator. https://www.digitalintelligence.com/products/forensic_duplicator/ Date of access: 1 Apr. 2016.

EC Council. 2004. Computer Hacking Forensic Investigator. Singapore: Thomson Learning.

Francoeur, J. 2003. The principles of electronic agreement legal admissibility. http://www.scribd.com/doc/276157/ The-Principles-of- Electronic-Agreement-Legal-Admissibility-WP-8-07 Date of access: 14 Jun. 2016.

Franklin, C. & Coustan, D. n.d. How operating systems work. How stuff work. http://computer.howstuffworks.com/operating-system.htm Date of access: 20 Dec. 2015.

Forensic Handbook. 2012. Locards Exchange Principle. http://www.forensichandbook.com/locards-exchange-principle/ Date of access: 16 Jul. 2016.

Galves, F. & Galves, C. 2004. Ensuring the admissibility of electronic forensic evidence and enhancing its probative value at trial. *Criminal Justice Magazine*, 19(1):3.

Gibson, W. 1984. Neuromancer. Washington: Phantasia Press.

Gookin, D. n.d. Understand how the Windows registry works. For dummies. http://www.dummies.com/how-to/content/understand-how-the-windows-registry-works.html Date of access: 22 Dec. 2015.

Guzzi, S. 2012. Digital searches and the Fourth Amendment: the interplay between the plain view doctrine and search-protocol warrant restrictions. *American Criminal Law Review*, 49(1):301-329.

Health and Safety Executive. 2014. Obtaining evidence using section 20 powers. http://www.hse.gov.uk/enforce/enforcementguide/investigation/physical-obtaining.htm. Date of access: 10 Aug. 2016.

Hart, H.L.A. 1958. Positivism and the separation of law and morals. *Harvard Law Review*, 71(4):607.

Hofman, J. 2006a. Electronic evidence in criminal cases. *South African Journal of Criminal Justice,* 19(3):257-275.

Hofman, J. 2006b. Electronic evidence in South Africa. http://hofman@law.uct.ac.za Date of access: 2 Nov. 2014.

Internet World Stats. 2015. http://www.internetworldstats.com/stats.htm Date of access:

International Organisation of Standardization. 2012. Information technology − Security techniques − Guidelines for identification, collection, acquisition, and preservation of digital evidence. Switzerland ISO/IEC (ISO/IEC DIS 27037).

International Organisation of Standardization. 2014. Information technology − Security techniques − Incident investigation principles and processes. Switzerland ISO/IEC (ISO/IEC DIS 27043).

Jain, M. 2015. Mobile companies launched three new phones every day in India last year. http://scroll.in/article/709543/mobile-companies-launched-three-new-phones-every-day-in-india-last-year Date of access: 10 May 2016.

Jopek-Bosiacka, A. 2011. Defining law terms: a cross-cultural perspective. https://www.degruyter.com/view/j/rela.2011.9.issue-1/v10015-011-0008-y/v10015-011-0008-y.xml Date of access: 5 Apr. 2016.

Kanellis, P. 2006. Digital crime and forensic science in cyberspace. London: Idea Group Inc.

Kessler, G. 2010. Judges' awareness, understanding, and application of digital evidence. Fort Lauderdale, Florida. Nova Southeastern University, Graduate School of Computer and Information Sciences. (Thesis − Phd).

Kerr, O.S. 2005a. Searches and seizures in a digital world. *Harvard Law Review*, 119(2):531-585.

Kerr, O.S. 2005b. Search warrants in an era of digital evidence. *Mississippi Law Journal*, 75(1):85-108.

Kerr, O.S. 2015. Executing warrants for digital evidence: The case for use restrictions on nonresponsive data. *Texas Tech Law Review*, 48(1):1.

Kraidy, M.M. 2008. The internet as a mass communication medium. Journalism and mass communication. http://www.eolss.net/sample-chapters/c04/e6-33-03.pdf Date of access: 5 Feb. 2016.

Lange, M.C.S. & Nimsger, K.M. 2004. Electronic evidence and discovery: What every lawyer should know. Chicago: ABA Publishing.

Law reports see Canada, New Zealand, South Africa & United States of America.

Legal Information Institute. n.d. Retrieved from https://www.law.cornell.edu/constitution/fourth_amendment

Lidbury, T. & Boland, M. 2012. Technology: Forensically sound collection of ESI. http://www.insidecounsel.com/2012/05/11/technology-forensically-sound-collection-of-esi Date of access: 13 Jan. 2016.

Losey, R. 2007. Ediscovery team blog. Hash. [Web blog post]. https://e-discoveryteam.com/school/computer-hash-5f0266c4c326b9a1ef9e39cb78c352dc/ Date of access: 16 Jul. 2016.

Lowenstein, A.S. 2007. Search and seizure on steroids: United States v. Comprehensive Drug Testing and its consequences for private information stored on commercial electronic databases. University of California, Los Angeles.

Lowe, D. n.d. Digital electronics: binary basics: electronics all-in-one for dummies. http://www.dummies.com/how-to/content/digital-electronics-binary-basics.html Date of access: 2 Sept. 2015.

McLain, G.R. 2007. United States v. Hill: a new rule, but no clarity for the rules governing computer searches and seizures. *George Mason Law Review,* 14(4):1071-1104.

McLeod, S. 2014. The interview method. http://www.simplypsychology.org/interviews.html Date of access: 3 Nov. 2016.

Mohay, G.M., Anderson, A., Collie, B., De Vel., O. & McKemmish, R.D. 2003. Computer and intrusion forensics. Boston: Artech House.

Mulazzani, M., Huber, M., & Weipple, E. n.d. Social network forensics: Tapping the data pool of social networks. http://www.sba-research.org/wp-content/uploads/publications/socialForensics_preprint.pdf Date of access: 5 May. 2005.

Neufeld, P.J. 2005. The (near) irrelevance of Daubert to criminal justice and some suggestions for reform. *American Journal of Public Health*, 95(S1):107-113.

New Zealand. 2006. Director of serious fraud office v A firm of solicitors 2006 (1) NZLR 586.

New Zealand. 2012. Search and Surveillance Act 24 of 2012.

Nieman, A. 2006. Search and seizure, production and preservation of electronic evidence. Tlokwe: NWU. (Thesis − PhD).

Nieman, A. 2009. Cyberforensics: bridging the law/technology divide. *Journal of Information, Law & Technology*, (1):1-29.

Occupytheory. 2014. Advantages and disadvantages of qualitative research. http://occupytheory.org/advantages-and-disadvantages-of-qualitative-research/ Date of access: 16 Jan. 2016.

Oxford English Dictionary. 2016. Computer. http://www.oxforddictionaries.com/definition/english/computer Date of access: 23 Apr. 2016.

Oxford English Dictionary. 2016. Cellular Phone. http://www.oxforddictionaries.com/definition/english/mobilecellulr-phone?q=mobile+phone Date of access: 23 Oct. 2016.

Oxford English Dictionary. 2016. Cyber. http://www.oxforddictionaries.com/definition/english/cyber?q=Cyber Date of access: 23 Oct. 2016.

Oxford English Dictionary. 2016. Search. http://www.oxforddictionaries.com/definition/english/search Date of access: 23 Oct. 2016.

Palmer, G. 2001. A road map for digital forensic research. Technical report DTR-T001-01, DFRWS, Report from the first digital forensic research workshop (DFRWS). https://isis.poly.edu/kulesh/forensics/docs/DFRWS_RM_Final.pdf Date of access: 10 Nov. 2015.

Pickering, S. 2009. Most concise description of cloud computing on the net. http://stephenpickering.com/2009/10/28/most_concise description_of_cloud_ computing_on_the_net Date of access: 20 Dec. 2016.

Pitt, W. 1763. The Elder. http://www.bartleby.com/100/248.html. Date of access: 5 Feb. 2015.

Plowden, P. & Stockdale, M. 1998. A picture is worth a thousand words. *New Law Journal*, 6833:432-437.

Resnik. D.B. 2015. What is ethics in research and why is it important? http://www.niehs.nih.gov/research/resources/bioethics/whatis/ Date of access: 1 Nov. 2016.

Ruhnkqa, J. & Bagby, J.W. 2008. Forensic implications of metadata in electronic files. *CPA Journal*, 78(6):68.

South African Police Service ***see*** South Africa. South African Police Service.

Sarkowicz, R. 1995. Levels of interpretation of a legal text. *Ratio Juris*, 8(1):104-112.

Schwikkard, P.J. & Van der Merwe, S.E. 2002. Principles of Evidence. 2nd ed. Cape Town: Juta.

Schneier, B. 1996. Applied cryptography, second edition protocols, algorithms and source code in C. New Jersey: John Wiley & Sons, Inc.

Schetina, E.S., Green, K. & Carlson, J. 2002. Internet site security. Boston: Addison- Wesley.

Scholtz, J. 2009. Towards an automated digital data forensic model with specific reference to investigation processes - A survey of actual and desirable practice. Auckland, New Zealand: Auckland University of Technology. (Thesis − Masters).

Seagate. 2016. Everything you wanted to know about hard drives. http://www.seagate.com/gb/en/do-more/everything-you-wanted-to-know-about-hard-drives-master-dm/ Date of access: 2 Feb. 2016.

Serra, F.A.R. 2015. Constructing a literature review. *Iberoamerican Journal of Strategic Management*, 14(3):1-5.

Silvernail, S.J. 1997. Electronic evidence: discovery in the computer age. *The Alabama Lawyer*, 58:176-177.

Smith, K. 2016. Marketing: 96 amazing social media statistics and facts for 2016. https://www.brandwatch.com/2016/03/96-amazing-social-media-statistics-and-facts-for-2016/ Date of access: 5 Apr. 2016.

South Africa. 1936. Scholsberg v. Attorney General of the Transvaal and the Additional Magistrate, Johannesburg: In re R v Sandig & others 1936 WLD 59.

South Africa. 1964. S v. Kearney 1964 (2) SA 495 (A).

South Africa. 1968. Heiman, Maasdorp and Barker v Secretary for Inland Revenue 1968 (4) SA 160 (W).

South Africa. 1976. Narlis v. South African Bank of Athens 1976 (2) SA 573 (A).

South Africa. 1977. Criminal Procedure Act 51 of 1977.

South Africa. 1981. Danzfuss v. Additional Magistrate, Bloemfontein, & Another 1981 (1) SA 115 (0).

South Africa. 1989. Smith, Tabata & Van Heerden Minister of Law & Order 1989 (3) SA 627 (E) 249.

South Africa. 1990. Naidoo & Another v. Minister of Law & Order & Another 1990 (2) SA 158 (W).

South Africa. 1990. Sasol (Edms) Bpk v. Minister van Wet en Orde 1991 (3) SA 766 (7) 33.

South Africa. 1992. Drugs and Drug Trafficking Act 140 of 1992.

South Africa. 1993. Bogoshi v. Van Vuuren NO; Bogoshi v Director Office of Serious Economic Offences 1993(3) SACR 98.

South Africa. 1995. Police Service Act 68 of 1995.

South Africa. 1995. S v. Makwanyane & another (CCT3/94) 1995 ZACC (3); 1995 (6) BCLR 665; 1995 (3) SA 391; 1996 (2) CHRLD 164; 1995 (2) SACR 1 (6 June 1995).

South Africa. 1995. Shabalala v. Attorney-General of Transvaal 1995 (2) SACR 761 (CC).

South Africa. 1996. Constitution of the Republic of South Africa.

South Africa. 1996. Rudolph v. Commissioner for Inland Revenue 1996 (7) BCLR 11 (CC).

South Africa. 1998. Competition Act 89 of 1998.

South Africa. 1998. National Prosecuting Act 32 of 1998.

South Africa. 2000. Investigating Directorate (2000): Serious Economic Offences v. Hyundai Motor Distributors (Pty) Ltd v. Smit.

South Africa. 2000. Ntoyakhe v. Minister of Safety and Security 2000 (1) SA 257 (E).

South Africa. 2000. Promotion of Access to Information Act 2 of 2000.

South Africa. 2002. Electronic Communication and Transaction Act 25 of 2002.

South Africa. 2002. Regulation of Interception of Communication and Provision of Communication-Related Information Act 70 of 2002.

South Africa. 2002. Smit & Maritz Attorneys and Another v. Lourens No and Others, 2002 (1) SACR 152.

South Africa. 2003. Minister of Safety and Security v. Xaba 2003 (1) All SA 596 (D).

South Africa. 2003. National Director of Public Prosecutions v Mohamed NO and Others (CCT44/02) 2003 ZACC 4; 2003 (1) SACR 561; 2003 (5) BCLR 476; 2003 (4) SA 1 (CC).

South Africa. 2004. Powell NO & Others v. Van der Merwe & Others (503/2002) 2004 ZASCA 25; 2005 (1) All SA 149 (SCA).

South Africa. 2004. Supreme Court of South Africa (SCSA). Beheersmaatscappij and Another v. The Magistrate Cape Town. (*In* The Supreme Court of South Africa (Cape Provincial Division): Case no. 5635 / 2004.

South Africa. 2005. Transvaal Provincial Division of the High Court. Case no. 10828/2005.

South Africa. 2006. Magajane v. Chairperson, North West Gambling Board (CCT49/05) 2006 ZACC 8; 2006 (10) BCLR 1133 (CC); 2006 (5) SA 250; 2006 (2) SACR 447.

South Africa. 2007. Minister of Safety and Security and Others v. Bennett and Others (302/06) 2007 ZASCA 136; 2007 SCA 136 (RSA); 2008 (2) All SA 26 (SCA); 2009 (2) SACR 17 (SCA).

South Africa. 2008. National Director of Public Prosecutions and Others v. Zuma and Another 2008 (1) All SA 197 (SCA).

South Africa. 2008. Ndiki 2008 (2) SACR 252 (Ck).

South Africa. 2008. Thint (Pty) Ltd v. National Director of Public Prosecutions and Others, Zuma and Another v. National Director of Public Prosecutions and Others (CCT 89/07, CCT 91/07) 2008 ZACC 13; 2008 (2) SACR 421 (CC); 2009 (1) SA 1 (CC); 2008 (12) BCLR 1197 (CC).

South Africa. 2010. Muller v. BOE Bank Ltd and Others (8723/98) 2010 ZAWCHC 121; 2011 (1) SA 252 (WCC); 2011 (1) All SA 166 (WCC).

South Africa. 2011. Minister for Safety and Security v. Van Der Merwe and Others (CCT90/10) 2011 ZACC 19; 2011 (5) SA 61 (CC); 2011 (9) BCLR 961 (CC); 2011 (2) SACR 301 (CC).

South Africa. 2011. Polonyfis v. Minister of Police and Others (64/10) 2011 ZASCA 26; 2012 (1) SACR 57 (SCA).

South Africa. 2012. Imperial Crown Trading 289 (Pty) Ltd v. Birch NO and Others (1338/2011) 2012 ZANCHC 12.

South Africa. 2013. Gaertner and Others v. Minister of Finance and Others 2013 (3) All SA 159 (WCC).

South Africa. 2016. Cybercrimes and Cybersecurity Bill. Document for submission to Cabinet.

South Africa. 2016. Goqwana v. Minister of Safety NO & Others (20668/2014) 2015 ZASCA 186; 2016 (1) All SA 629 (SCA); 2016 (1) SACR 384 (SCA).

South Africa. 2016. Gumede v. S (800/2015) 2016 ZASCA 148.

South Africa. 2016. Heaney v. S (A464/2015) 2016 ZAGPPHC 257.

South Africa. 2016. Minister of Police and Others v Kunjana (CCT253/15) 2016 ZACC 21.

South Africa. SAPS. 2002. National Instruction 2/2002, search and seizure. Pretoria.

South Africa. SAPS. 2016. 2016 Crime Stats Presentation. Pretoria.

South Africa. SAPS. 2016. Practical Guide to Apply for Search Warrants in terms of Section 21 of the Criminal Procedure Act 51 of 1977. Pretoria.

South Africa. SAPS. 2016. Interim Standing Operating Procedures dealing with Electronic Evidence. Pretoria.

South African Law Reform Commission. 2002. Discussion Paper, 99, on Computer Generated Crime. Pretoria.

South African Law Reform Commission. 2005. Discussion Paper, 109, Privacy and Data Protection. Pretoria.

South African Law Reform Commission. 2010. Issue Paper 27, Project 126 Review of the Law of Evidence Electronic Evidence in Criminal and Civil Proceedings: Admissibility and Related Issues. Pretoria

Spencer, M. 2014. What's the difference between "electronic" and "digital"? https://www.quora.com/Whats-the-difference-between-electronic-and-digital Date of access: 23 May 2016.

Sravani, S. 2016. Unstructured interviews: definition, advantages and disadvantages. http://content.wisestep.com/unstructured-interview-definition-advantages-disadvantages/ Date of access: 2 Nov. 2016.

Statista. 2016. Number of mobile phone users worldwide from 2013 to 2019. http://www.statista.com/statistics/274774/forecast-of-mobile-phone-users-worldwide/ Date of access: 3 Jun. 2016.

Steytler, N. 2004. Constitutional Criminal Procedure − a commentary on the Constitution of the Republic of South Africa. Durban: Butterworths.

Scientific Working Group on Digital Evidence. 2012. SWGDE and SWGIT Digital & Multimedia Evidence Glossary. https://www.swgit.org/pdf/SWGDE%20and%20SWGIT%20Digital%20and%20Multimedia%20Evidence%20Glossary?docID=60 Date of access: 3 May 2015.

The Forensic Library. 2014. Edmond Locard. http://aboutforensics.co.uk/edmond-locard/ Date of access: 12 Dec. 2015.

Terre Blanche, M., Durrheim. K. & Painter, D. 2010. Research in Practise. Cape Town: UCT Press.

Thompson, E. 2005. MD5 collisions and the impact on computer forensics. *Digital Investigation*, 2(1):36-40.

United Kingdom. 2001. Criminal Justice and Police Act 16 of 2001.

United Nations. 1996. United Nation's Commission on International Trade Law's (UNICITRAL) Model Law on Electronic Commerce with Guide to Enhancement. https://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf Date of access: 23 Nov. 2015.

United States of America. 1982. United States v. Tamura, 694 F.2d 591 (9th Cir. 1982).

United States of America. 1987. Arizona v. Hicks, 480 U.S. 321, 325 (1987).

United States of America. 1993. Daubert v. Merrell Dow Pharmaceuticals, Inc. (92-102), 509 U.S. 579 (1993).

United States of America. 1997. Davis v. Gracey, 111 F.3d 1472 (10th Cir. 1997).

United States of America. 1999. United States v. Ford, 184 F.3d 566 (6th Cir. 1999).

United States of America. 2000. United States v. Hay, 231 F.3d 630 (9th Cir. 2000).

United States of America. 2002. United States v. Hernandez, 183 F. Supp.2d 468, 480-81 (D.P.R. 2002).

United States of America. 2002. United States v. Triumph Capital Grp., Inc., 211 F.R.D. 31, 66 (D. Conn. 2002).

United States of America. 2004. United States v. Gorrell, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004).

United States of America. 2005. United States v. Syphers, 426 F.3d 461, 469 (1st Cir. 2005).

United States of America. 2006. United States v. Comprehensive Drug Testing, Inc., 473 F.3d 915, 920 (9th Cir. 2006).

United States of America. 2006. United States v. Hill, 459 F.3d 966, 977-78 (9th Cir. 2006).

United States of America. 2007. Lorraine v. Markel American Ins. Co. (2007), 241 F.R.D. 534, 544 (D. Md. 2007).

United States of America. 2007. United States v. Fleet Management Ltd., 521 F. Supp. 2d 436 (E.D. Pa. 2007).

United States of America. 2007. United States v. Vilar, 2007 U.S. Dist. LEXIS 26993, 124-25 (S.D.N.Y. 2007.

United States of America. 2009. Federal Rules of Criminal Procedure Rule 41, Search and Seizure.

United States of America. 2009. United States v. Brewer, 588 F.3d 1165, 1173 (8th Cir. 2009).

United States of America. 2009. United States v. Burgess, 576 F.3d 1078, 1082 (10th Cir. 2009).

United States of America. 2009. United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989, 1006-07 (9th Cir. 2009) (en banc).

United States of America. 2010. United States v. Comprehensive Drug Testing, Inc., Nos. 05-10067, 05-15006, 05-55354, 2010 WL 3529247 (9th Cir. Sept. 13, 2010), revising and super ceding 579 F.3d at 989.

United States of America. 2010. United States v. Mann, 592 F.3d 779, 786 (7th Cir. 2010).

United States of America. 2011. United States District Court (USDC) (2011). The Matter of the United States of America's Application for a Search Warrant to Seize Electronic Devices from Edward Cunnius.

United States of America. 2012. United States v. Flores-Lopez, No. 10-3803 (7th Cir. 2012).

United States of America. 2012. United States v. Metter, [no.10-CR-600 (E.D.N.Y. 05/17/2012)].

United States of America. Constitution. Fourth. https://www.law.cornell.edu/constitution/fourth_amendment Date of access: 15 Oct. 2016.

United States of America. Department of Justice. 2004. Forensic Examination of digital evidence: A guide for Law enforcement.

United States of America. Department of Justice. 2009. Searching and seizing computers and obtaining electronic evidence in criminal investigations. US Department of Justice.

US-Cert. 2005. Digital Forensics. https://www.us-cert.gov/sites/default/files/publications/forensics.pdf Date of access: 15 Oct. 2016.

Vacca, J.R. 2005. Computer forensics computer crime scene investigation. 2nd ed. Massachusetts: Charles River Media Inc.

Van Buskkirk, E. & Liu, V.T. 2006. Digital evidence: Challenging the presumption of reliability. *Journal of Digital Forensic Practice*, 1(1):25.

Van der Merwe, D., Roos, A., Pistorius, T. & Eiselen, S. 2008. Information and communications technology law. Durban: LexisNexis.

Van Deusen Phillips, S. 2010. The Documentalist - Legal Considerations for Electronic Evidence, Part 5: Original vs. Duplicate Documents & Unfair Prejudice accessed. [Web log post]. https://crlgrn.wordpress.com/2010/07/27/legal-considerations-for-electronic-evidence-part-5-original-vs-duplicate-documents-unfair-prejudice/ Date of access: 23 Oct. 2015.

Vandeven, S. 2014. Forensic images: for your viewing pleasure. https://www.sans.org/reading-room/whitepapers/forensics/forensic-images-viewing-pleasure-35447 Date of access: 2 Oct. 2015.

Wang, S.J. 2007. Measures of retaining digital evidence to prosecute computer based cybercrimes. *Computer Standards & Interfaces*, 29(2):8.

Webster, J. & Watson, R. 2002. Analyse the past to prepare for the future: writing a literary review. *MIS Quarterly*, 26(2):xIII-xxIII.

Welty, J. 2011. Warrant searches of computers. Spring Public Defender and Investigator Conference organised by NCIDS.

http://www.ncids.org/Defender%20Training/Training%20Index.htm Date of access: 2 Nov. 2015.

Winick, R. 1994. Searches and seizures of computers and computer data. http://jolt.law.harvard.edu/articles/pdf/v08/08HarvJLTech075.pdf Date of access: 12 Nov. 2015.

Woodford, C. 2007. Computers. Explain that stuff. http://www.explainthatstuff.com/howcomputerswork.html Date of access: 22 Feb. 2016.

Wyse, S.E. 2011. What is the difference between qualitative research and quantitative research? http://www.snapsurveys.com/blog/what-is-the-difference-between-qualitative-research-and-quantitative-research/ Date of access: 10 Nov. 2015.